PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G10L 5/06	A1	(11) International Publication Number: WO 99/22362
		(43) International Publication Date: 6 May 1999 (06.05.99)

(21) International Application Number: PCT/IB98/01835

(22) International Filing Date: 26 October 1998 (26.10.98)

(30) Priority Data:
122023 26 October 1997 (26.10.97) IL

(71) Applicant *(for all designated States except US)*: ENCO-TONE LTD. [IL/IL]; P.O. Box 45094, 91450 Jerusalem (IL).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: LABATON, Isaac, J. [IL/IL]; P.O. Box 45094, 91450 Jerusalem (IL).

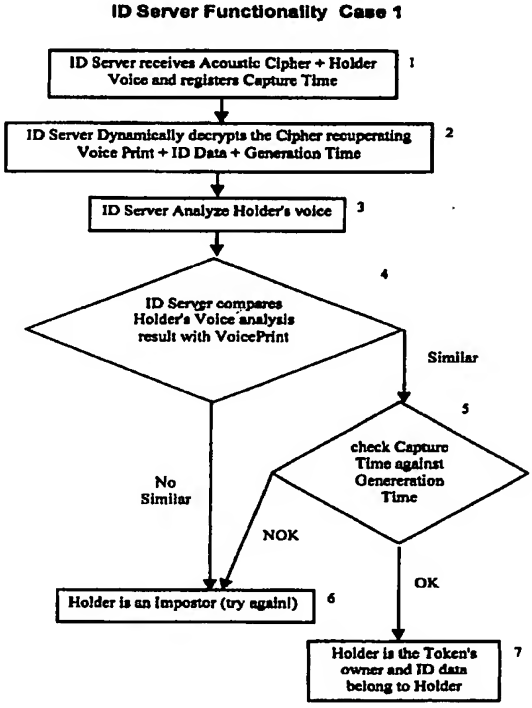
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: NON-TRANSFERABLE BIO-METRIC TOKEN-BASED IDENTIFICATION METHODS AND DEVICES

(57) Abstract

A person's voice input is received (1) and analyzed (3). A comparison is made to a stored voice print (4). The result of the comparison indicates whether the person is an impostor (6) or is a valid holder of a portable device.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

NON-TRANSFERABLE BIO-METRIC TOKEN-BASED IDENTIFICATION METHODS AND DEVICES

TECHNICAL FIELD

The present invention relates, generally, to systems, methods and apparatus for personal identification.

BACKGROUND OF THE INVENTION

Voice analysis, characterization and recognition technology is a mature field and is referred to herein as Speaker (identity) Verification Software (SVS) and the Speaker Verification Application Programming Interface (SVAPI) projected standard.

Use of these current voice characterization and recognition technologies for personal identification purposes has several problems. First, the percentage of error in voice identification, estimated to be approximately 3%, is not reliable enough for use in financial transactions. Second, current identification devices require the use of a database wherein each person's voice characteristic (referred to hereinafter as a Voice Print) is stored for comparison purposes. The need to store such information at the identification device necessarily limits the use of current technology for some applications. Accordingly, there is a need for new systems, methods and apparatus which will improve substantially the reliability of personal identification using voice recognition technology, and further will alleviate the need to store voice characteristic data at the decryption or identification device.

BRIEF SUMMARY OF THE INVENTION

It is an object of the present invention to provide methods and apparatus which will improve substantially the reliability of personal identification using voice

recognition technology, and further will alleviate the need to store voice characteristic data at the decryption or identification device.

The present invention comprises devices including, but not limited to, a Personalization Machine; a Bio-Token (non-transferable electronic portable device) carried by a person (carrier) to be identified either as the owner/rightful possessor of the Bio-Token or not, which stores the owner's Voice Print or, alternatively, a chip (e.g., in a cellular phone or other device) or a chip card which stores the same; and/or an Identification Device (e.g., an ID server) which may receive the Voice Print from the Token and the actual voice (utterance) of the Bio-Token's carrier (person carrying the Bio-Token or other Voice Print storage device). The invention also may comprise any of several device variations described below.

The invention further comprises a number of methods designed to provide for the identification of a person holding a portable device referred to as a Bio-Token, as being either the owner/rightful possessor or not, as well as methods for certification of voice documents.

One method encompassed by the present invention preferably comprises the use of Speaker Verification Software, which is commercially available, to obtain the Voice Print of the rightful owner of the portable device (Bio-Token). The method further preferably comprises a step of providing the owner's identification data to the Bio-Token device (see FIG. 1), which may include his or her name and/or address, and/or driver license, and/or passport number, and/or any identity card, and/or transaction data, and/or amounts of money, like the credit limits (for Debit Card usage) and/or any other information useful to a particular transaction requiring reliable owner identification. The method also may comprise an optional step of encrypting the Voice Print and the owner's identification data, such encryption step referred to hereinafter as Static Encryption. The method further may comprise a step of storing into the Bio-Token device carried by the person to be identified (carrier/holder), the carrier's Voice Print, Identification Data and/or Static Encryption results. The above steps may be referred to in part or as a whole as a Personalization Procedure.

The methods of the invention further may comprise a step of distributing Identification Devices and/or Identification Software. The same Speaker Verification

Software previously used to create the Voice Print during the Personalization Procedure may be installed in such Identification Devices, each Identification Device thereby having the operational capability to decrypt Voice Prints and/or Identification Data. Of course, such Identification Devices alternatively may use any other suitable software or hardware to decrypt Voice Prints and/or identification data.

The present invention further encompasses methods for identification. Each time that a carrier of a portable device (Bio-Token) needs to be identified, the carrier may activate the Bio-Token device. Activation may require that the carrier first enter a PIN into the Bio-Token device. Once activated, the Bio-Token device then may read from its electronic memory the Voice Print of the rightful owner, previously entered, and then may merge or concatenate such digits with a time stamp or use any other method in order to create a dynamic message (such as a sequential method), wherein the dynamic message is encrypted (referred to hereinafter as Dynamic Encryption) by the Bio-Token, the result of such Dynamic Encryption referred to hereinafter as a Cipher. The method also may include an optional step of encoding the Cipher into sound, in which case an Acoustic Message produced by the Bio-Token may be referred to as an Acoustic Cipher.

Both the audio signals of the Acoustic Cipher (Acoustic Message) and the actual voice (utterance) of the carrier (referred to hereinafter as the Voice String) then may be transmitted to the Identification Device. The transmission may be made directly or indirectly, e.g., transmitted by any media of communication such as phone, Internet, data transmission lines, etc. eventually reaching, on-line or off-line, an Identification Device.

The Cipher, encoded or not, should reach an Identification Device, on-line or off-line, together with the actual voice utterance (Voice String) of the Bio-Token's carrier. In a preferred embodiment of the present invention, the Voice String may be transmitted in the form of an answer to a variable question or request, e.g., "Please repeat the words: Bill Clinton," or " Say the date and time in minutes, hours, days and years," or "Please say the transaction data, if any, to be certified by this identification."

The methods of the present invention also may comprise a step of decrypting the cipher received by the Identification Device. The Identification Device decrypts the cipher (Dynamic Decryption), thereby obtaining the Statically Encrypted Voice Print and, then, Statically Decrypts the Statically Encrypted Voice Print to recuperate the Voice Print (referred to herein as the "Computed Result").

The methods of this invention also may include the step of analyzing the Voice String received by the Identification Device, preferably by means of Speaker (identity) Verification Software, and then comparing such analysis results with the Computed Result.

Naturally, if both results are similar, within a pre-established tolerance, the Identification Device then may conclude that the rightful Owner of the portable device (Bio-Token) is the present Carrier of the Bio-Token, whose voice response has been analyzed. Due to the fact that the Cipher also includes the authorized owner's ID Data and/or the transaction data, such as his name, and/or address, and/or driver license and/or passport number, etc., the Identification Device will have the ID Data certified with some certainty that the data corresponds to the present Carrier of the Bio-Token and thereby helping to avoid the possibility that the Carrier is an impostor.

In accordance with a further aspect of the present invention, an alternative method for remote identification is provided wherein the Bio-Token generates a scrambled sample of the Owner's voice. More precisely, the Bio-Token may reproduce a sample of the Owner's voice which was pre-recorded by the Personalization Machine and stored into the Bio-Token during the Personalization Procedure. This sample may be scrambled, before being converted into sound, by mixing it with an encoded number. The encoded number preferably is a variable number, with a very large cycle for repetitions, referred to hereinafter as a pseudo-random number. The Owner's voice sample mixed with the pseudo-random number is referred to hereinafter as a Scrambled Owner Voice Sample.

With respect to this alternative aspect of the present invention, each time a Bio-Token's carrier needs to identify his or herself to an Identification Device, the Bio-Token may compute a new dynamic password or digital signature. The dynamic password/digital signature then preferably is embedded with the Owner's ID Data and

the data preferably is used as a "seed" to compute the pseudo random number for scrambling purposes.

The Bio-Token may then encode the dynamic password/digital signature and scrambled Owner's Voice Sample into sound, referred to hereinafter as a Scrambled Acoustic Message. This Scrambled Acoustic Message may then be transmitted, directly or indirectly, to the Identification Device together with the Carrier's voice (Voice String) as described above. Preferably, the Voice String comprises the same words or phrase as the Owner's Voice Sample. The Identification Device may then decode the dynamic password/digital signature and decrypt it, recuperating the Owner's ID Data and the Seed. The Seed then preferably is used by the Identification Device to compute the pseudo random number and, with such information, de-scramble the received scrambled Owner's Voice Sample thereby recuperating the Owner's voice sample. The Identification Device then may analyze the sample together with the carrier's Voice Sample, by means of Speaker Verification Software, and conclude whether they are similar or not. In a positive case, the Identification Device may display or transmit the owner's received ID Data.

The present invention further may comprise a number of suitable devices such as Personalization Machines, a multitude of Bio-Token devices, and a multitude of Identification Devices (e.g., ID Servers). Preferably, a Personalization Machine is a machine capable of reading from one or more media, for example, Hard Disks, floppy disks, RAM, ROM, Dangles, PCMCIA, Chip cards or others; recording and analyzing voice samples, e.g., running Speaker (identity) Verification Software; generating Voice Prints; elaborating Voice Prints; and writing into the electronic memory of a Bio-Token device.

Preferably, Bio-Token devices are portable electronic devices with memory, having the capability to read from the memory, to compute, to encrypt, and to encode results into sound.

The Identification Devices preferably are devices capable of reading from one or several media, e.g., Hard Disks, floppy disks, RAM, ROM, Dangles, PCMCIA, Chip cards or others; recording, digitizing and analyzing voice samples, e.g., running Speaker (identity) Verification Software; generating Voice Prints; elaborating Voice

Prints; and/or recording, digitizing and analyzing Acoustic Messages generated by the Bio-Token devices, including Acoustic Ciphers.

BRIEF DESCRIPTION OF THE DRAWINGS

The subject invention will hereinafter be described in conjunction with the appended drawing figures:

Fig. 1 is a block flow diagram representing the functionality of the Personalization Machine (PM) for one particular case referred in the following;

Fig . 2 is a block flow diagram representing the functionality of the Personalization Machine (PM) for another case referred in the following, which includes Static Encryption;

Fig. 3 is a block flow diagram representing the functionality of the Bio-Token device for another case referred in the following;

Fig. 4 is a block flow diagram representing the functionality of the Bio-Token device for another case referred in the following which includes Static Encryption;

Fig. 5 is a block flow diagram representing the functionality of the Bio-Token device for another case referred in the following, which includes Static Encryption and further includes the generation of calibration signals to correct distortion effects;

Fig. 6 is a block flow diagram representing the functionality if the Identification Device;

Fig. 7 is a block flow diagram representing the functionality of the Identification Device with Static Encryption;

Fig. 8 is a block flow diagram representing the functionality of the Identification Device with Static Encryption and further including the use of calibration signals to correct distortion effects;

Fig. 9 is a block flow diagram representing the Identification Process, including Bio-Token and Identification Device functionality;

Fig. 10 is a block flow diagram representing the Identification Process, including Bio-Token and Identification Device functionality, wherein the Identification Device reads secrets keys from a chip-card;

Fig. 11 is a block flow diagram representing the Identification Process, including Bio-Token and Identification Device functionality, wherein the Identification Device reads the secrets keys from a chip-card and performs Static decryption;

Fig. 12 is a block flow diagram representing the functionality of the invention wherein the Bio-Token is implemented in a cellular phone to eliminate the cloning fraud;

Fig. 13 is a block flow diagram of the functionality of the invention wherein the Bio-Token is implemented in a Debit-Card;

Fig. 14 is a block diagram of the Bio-Token/ROV-Bio-Token components;

Fig. 15 is a block flow diagram representing the functionality of the invention wherein the Bio-Token is implemented in one type of Travelers Check application;

Fig. 16 is a block flow diagram representing the functionality of the invention wherein the Bio-Token is implemented in one type of Debit-Card application;

Fig. 17 is a block flow diagram representing the functionality of the invention wherein the Bio-Token is implemented in one type of Debit-Card application;

Fig. 18 is a block flow diagram representing the functionality of a Personalization Machine for use with an ROV-Bio-Token, Static Encryption is not shown in order to simplify the diagram;

Fig. 19 is a block flow diagram representing the functionality of an ROV-Bio-Token, Static Encryption is not shown in order to simplify the diagram;

Fig. 20 is a block flow diagram representing the steps for scrambling a Real Owner's Voice (ROV) specimen, specifically, the computation of the samples of the SN;

Fig. 21 is a block flow diagram representing the functionality of an Identification Device for use with an ROV-Bio-Token, Static Encryption is not shown in order to simplify the diagram;

Fig. 22 is a block flow diagram representing the steps for descrambling the Real Owner's Voice (ROV) specimen, and specifically, the computation of the samples of the SN at the Identification Device; and

Fig. 23 is a block flow diagram representing the functionality of the invention wherein an ROV-Bio-Token is implemented in a cellular phone to protect against cloning, Static Encryption is not shown in order to simplify the diagram.

DETAILED DESCRIPTION

While a number of preferred embodiments of the present invention will be described in detail herein, the present invention more generally encompasses remote identification systems, methods and devices which allow the identity of a person ("Owner") to be compared to that of a holder ("Holder" or "Carrier") of a portable device ("Bio-Token"). Identification may be performed by a remote device ("Identification Device") by comparing a voice sample characteristic stored in the Bio-Token to a characteristic of a real voice sample ("Utterance") provided by the carrier of the Bio-Token, thereby determining whether the Holder of the Bio-Token is indeed the Owner. The methods of the present invention may further allow for the certification of such Utterances.

In general, the methods associated with the present invention preferably comprise some or all of the following steps (see Fig. 1): personalizing the Bio-Token, comprising the following sub-steps:

Step 1: connecting the Bio-Token to a specific machine referred to as a Personalization Machine (PM);

Step 2: entering a set of the Owner's ID Data into the PM;

Step 3: capturing a sample of the Owner's voice and generating a Voice Print from the Owner's voice sample, preferably by means of commercially available speech recognition software or Speaker Verification Software;

Step 4: writing or registering into the Bio-Token's memory the Owner's Identification Data and Voice Print, or, optionally, registering such information on a chip-card which then can be inserted into the Token; and properly identifying whether the Holder of a Bio-Token is the owner, by an Identification Device (e.g., ID Server) (see Figs. 9 and 10), preferably comprising some or all of the following sub-steps:

a) the Bio-Token's Holder actuates the Bio-Token;

b) the Holder provides an Utterance to the Identification Device;

c) the Identification Device receives an Acoustic Message generated by the Bio-Token, along with the Holder's voice (Utterance) (see Fig. 6);

d) the Identification Device compares the Voice Print in the Acoustic Message provided by the Bio-Token to a voice print of the Utterance.

Referring now to Fig. 3, a preferred embodiment of a Bio-Token will be described. When a Bio-Token is switched on, the Holder may be prompted to enter a Personal Identification Number (optional). Once the Bio-Token is on and operational, it may read the Owner's Voice Print and/or Identification Data from memory, or, alternatively, from a chip card where the Voice Print and/or the Owner's ID Data are stored. The Bio-Token then preferably encrypts the Voice Print, the Owner's Identification Data and the Generation Time (e.g., present GMT time and date) into a Cipher, in a manner such that each and any Cipher is distinct from the previous one, and the repetition cycle is very large (e.g., tens of years). A preferred encryption scheme is described in U.S. Patent No. 5,524,072 (PCT/US92/10492), but any suitable encryption scheme may be utilized. This encryption step will be referred to herein as "Dynamic Encryption" (see Fig. 3, Step 4). Optionally, the Token can encode the Cipher into sound using MODEM techniques or any other method of encoding digits into sound (see Fig. 3, Steps 5 and 6), in which case an Acoustic Message produced by the Bio-Token may be referred to as an "Acoustic Cipher."

Referring now to Fig. 6, preferred methods of Holder identification will now be described. As shown in Step 1, an Identification Device (e.g., ID Server) preferably receives an Acoustic Message from the Bio-Token along with the Holder's voice ("Utterance"), and registers the time of arrival ("Capture Time") of such Acoustic Message. As illustrated in Step 2, the Identification Device suitably decrypts the Dynamic Encryption thereby recapturing the Voice Print, the Identification Data and the Generation Time. As shown in Step 3, the Identification Device may then analyze the Holder's utterance by means of any suitable software (such software is already commercially available). In Step 4, the Identification Device may then compare the Voice Print, received within the Cipher, to the results of the analysis. If the Voice Print is similar to the results of the Utterance analysis, within pre-established

tolerances, then, as shown in Step 5, the Identification Device preferably goes on to check the Capture Time against the recaptured Generation Time to avoid intercepted Acoustic Messages. If OK, the Identification Device has identified and authenticated the Holder and may then proceed with a particular transaction, e.g., with the display and/or transmission of the Owner's Identification Data.

In a further exemplary embodiment of the present invention, methods are provided which allow for the personal identification of a person holding a Bio-Token, which further include the certification of voice documents. Preferably, these methods comprise the step of personalizing the Bio-Token, which preferably comprises one or more of the following sub-steps (see Fig. 2):

Step 1: loading the Personalization Machine with encryption keys;

Step 2: entering the Bio-Token on the Personalization Machine,

Step 3: entering the Owner's Identification Data,

Step 4: capturing the Owner's voice, generating the Voice Print, and, optionally, compressing, and/or mathematically elaborating such Voice Print (e.g., averaging or/and hashing the Voice Print); and

Step 5: Statically Encrypting the Voice Print and/or the Identification Data, using system keys. For example, a system's private key may be used to encrypt the Voice Print. Furthermore, a private key (for example, a key referred to herein as SSPrK#I) may be used to encrypt the Owner's name and address; a private key (for example, a key referred to herein as SSPrK#2) may be used to encrypt the Owner's Driver license data; a private key (for example, a key referred to herein as SSPrK#3) may be used to encrypt the Owner's passport data; a private key (for example, a key referred to herein as SSPrK#4) may be used to encrypt the Owner's Credit Card data; a private key (for example, referred to herein as SSPrK#5) may be used to encode the owner's Social Security number; and so on, any appropriate number of keys (e.g., SSPr#n) may be used to encrypt whatever data about the Owner that may be pertinent.

Step 6: writing or registering into the Bio-Token memory the Statically Encrypted Owner's Identification Data and Voice Print.

Because the encryption described in Step 5 differs fundamentally from the above-described Dynamic Encryption (the encryption of Step 5 is fixed, with no time variable), this step is referred to herein as Static Encryption. Accordingly, any keys utilized by the Static Encryption are referred to herein as Static Encryption Keys.

These methods further may comprise the step of properly identifying the Holder of the Bio-Token by the Identification Device, preferably comprising one or more of the following sub-steps (see Fig. 11):

a) the Token's Holder actuates the Bio-Token (see Fig. 4) and the Bio-Token transmits an Acoustic Cipher to the Identification Device;

b) the Holder speaks (transmits an Utterance to the Identification Device); and

c) the Identification Device receives the Acoustic Message generated by the Bio-Token and the Holder's voice (see Fig. 7).

Now referring to Fig. 4, when a Bio-Token is switched on, the Holder may be required to enter a Personal Identification Number (optional). Once the Bio-Token is on and functional, it may then read the Statically Encrypted Voice Print and/or Statically Encrypted Owner's Identification Data from the Bio-Token's memory or, alternatively, from a chip card where the Voice Print and/or the Owner's Identification Data are stored. The Bio-Token may then Dynamically encrypt the Voice Print, the Owner's Identification Data and the Generation Time, as discussed above, into a Cipher. Optionally, the Token may then encode the Cipher into sound, in which case an Acoustic Message produced by the Bio-Token may be referred to as an Acoustic Cipher.

Referring now to the Identification Device (e.g., ID Server) functionality, the following steps preferably are performed (see Fig. 7):

Step 1: the Identification Device (e.g., ID Server) receives the Acoustic Message from the Bio-Token, along with the Holder's utterance, and registers the Capture Time;

Step 2: the Identification Device decrypts the Dynamic Encryption, recuperating the Statically Encrypted Voice Print, Identification Data and Generation Time;

Step 3: the Identification Device decrypts the Statically Encrypted Voice Print (e.g., using the system's respective public key);

Step 4: the Identification Device analyzes the Holder's voice (Utterance);

Step 5: the Identification Device compares the Voice Print with the results of the analysis of the Holder's voice (Utterance);

Step 6: if the Voice Print is similar to the analysis of the Holder's voice, within pre-established tolerances, then the Identification Device preferably goes on to check the Capture Time against the recuperated Generation Time, to avoid intercepted Acoustic Messages; and

Step 7: if OK, the Identification Device preferably proceeds with the transaction, e.g., to Statically Decrypt the Owner's Identification Data, as described below.

To Statically decrypt the Owner's Identification Data, the Identification Device preferably uses the corresponding key (i.e. the public key to SSPr#j j=l,,,n)) , according to the particular Identification Device's level of data accessibility and/or keys availability. For example, a Police Department's ID Servers may have all the public keys and, therefore, will be able to Statically decrypt any and all of the Owner's Identification Data. On the other hand, an Identification Device of lower accessability may hold only a limited number of public keys, for example, a system may only hold Public Keys #1 and 2 (referred to above SSPuK#l and SSPuK#2). In that case, the Identification Device will only be able to decrypt two pieces of the Owner's Identification Data, e.g., the Owner's name and address (using SSPuK#l) and the Owner's Driver license (using the public key referred as SSPuK#2)). The method also preferably includes the optional step of displaying or/and transmitting the Statically Decrypted portion of the Owner's ID Data.

In accordance with another aspect of the present invention, methods and apparatus are provided for remote identification wherein the Bio-Token can store and scramble a specific Owner's voice specimen. In accordance with this particular embodiment of the invention, the Bio-Token is referred to as the Real Owner's Voice (ROV) Storing and Scrambling Token, or ROV-Bio-Token. The ROV-Bio-Token preferably is capable of reproducing a specimen of the Owner's voice, which was

pre-recorded by the PM (Personalization Machine) and stored in the ROV-Bio-Token during the personalization procedure (see Fig. 18, the optional Static Encryption was not included in this diagram to simplify the explanation). The Real Owner's Voice specimen may be scrambled, resulting in a "Scrambled ROV Specimen," before being reproduced by the ROV-Bio-Token.

The above-mentioned scrambling step preferably is a variable-result-scrambling-step, which helps to avoid misuse or fraud, e.g., the recording and subsequent usage of the Scrambled Real Owner's Voice specimen in order to impersonate the Owner. With respect to this aspect of the invention, in spite of the fact that the Real Owner's Voice specimen is constant, the Scrambled ROV Voice specimen becomes obsolete soon after being reproduced by the ROV-Bio-Token due to the fact that is scrambled using a different scrambling factor each time, each factor becoming obsolete soon after its use.

More precisely, the Real Owner's Voice specimen may be stored in the token's memory as digits (samples), these samples preferably being the result of the digitization made in the Personalization Machine. Then, a variable number (referred as the Scrambling Number or SN) may be computed by the token's CPU and converted into digits as a first step towards its encodification into sound, (referred to herein as "SN Samples"). After being converted, the SN Samples will become a large set of hex-digits which represents the analog wave sound samples, such as would be obtained if the SN were in DTMF tones and being digitized (a possible method for accomplishing such conversion in a chip is described in a 1993 document of Microchip Technology Inc referred as AN543).

In order to further clarify this scrambling aspect of this invention, and referring now to Figs. 20 and 22, assume, for example, that we are after the computation of the variable number SN in hex-digits, i.e.: SN = 567fa34590b5278c7ff45639a567fa34590b5278c7ff45639a. Each one of the numbers will be converted by the Bio-Token into a concatenation of digits (Samples, referred to herein as SN Samples), wherein each digit represents the amplitude of the analog sound wave sample resulting from the conversion of the number into DTMF. Following with the example, the first digit of SN, the number 5, can be converted into

a sound wave, according to the DTMF standard, which consists of 2 frequencies f_1 and f_2,

$$5 \text{ Converted to} \rightarrow A \sin(2\pi f_1 t + \varphi_1) + B \sin(2\pi f_2 t + \varphi_2)$$

with a duration of 75 milliseconds and a pause of 10 milliseconds. Therefore, if the sampling rate is 8000 samples per second, the "digitation of the number" will consist of 680 samples (hex-digits).

If this process is repeated for each one of the 50 numbers constituting SN, we will have 34000 samples, totaling 4.25 seconds. Using this method or a similar method, the digitized Real Owner's Voice specimen is scrambled using the 34000 samples, periodically, that is, for each 4.25 sec of the duration of the Real Owner's Voice specimen, before being converted into sound by the Bio-Token . As an example, a scrambling procedure can be as simple as summing the corresponding samples of the specimen and SN samples:

Scrambled ROV Specimen Sample(i) = ***ROV Specimen Sample(i)*** + ***SN Sample (i)***,

and like this for each *i*, from 1 to 34000, and starting again if the duration of the Real Owner's Voice specimen, is more than 4.25 sec.

Accordingly, the scrambling procedure may be accomplished by the superposition of the specimen with an encoded number. For example, the two sets of numbers may be summed, sample by sample, wherein one of the said sets represents a received and digitized Scrambled Real Owner's Voice specimen Samples and the other set represents the Scrambling Number samples, preferably, but not necessary, made with the same sampling rate (i.e.: 8000 samples/sec) (see Fig. 20).

One fundamental aspect of the above-mentioned method is that in spite of the fact that the Real Owner's Voice specimen, stored in the Bio-Token, is a constant and non-timely variable, the Scrambled Real Owner's Voice specimen is constantly variable and will never repeat over a large period of time. Further, due to the fact that the Dynamic Message, which is concatenated with the Scrambled Real Owner's Voice specimen, also carries the Generation time and date, the recording and subsequent usage of the Acoustic message is prevented.

The ROV-Bio-Token may compute the SN from a Seed number, creating a distinct number each time, and then embed and transmit the Seed number with the Acoustic Message in a manner which will allow the ROV-Identification-Device (e.g., ROV-ID-Server) to recuperate the Seed and re-compute the SN. The data needed to compute the Scrambling Number is referred to herein as the "Scrambling Number's Seed," or just "Seed."

The ROV-Identification Device, having re-computed the SN (see Fig. 22), then may compute the SN Samples, deducting such samples from the received and digitized Scrambled Real Owner's Voice specimen Samples and, with them, recapture the Real Owner's Voice specimen Samples,

e.g., ***ROV Specimen Sample(i)*** = ***Scrambled ROV Specimen Sample(i)*** - ***SN Sample (i).***

Having recuperated the Real Owner's Voice specimen Samples, the ROV-Identification device may continue with the Identification procedure as described in the block flow diagram shown in Fig. 21. All of the numbers and methods of scrambling described above are merely exemplary, and that any suitable scrambling methods will suffice.

According to another aspect of the present invention, modem technology may be utilized to transmit the Acoustic Message, wherein the scrambling procedure may comprise the XORing of the ROV Specimen samples with the SN samples. Referring again to Fig. 21, an utterance reproduced by the Bio-Token may be transmitted to the Identification Device (e.g., ID server) where it may then be recorded and unscrambled. More precisely, and according to this aspect of the present invention, each time the ROV-Bio-Token Holder needs to identify himself to the ROV-Identification Device, the ROV-Bio-Token may compute a new Dynamic Message, which carries embedded in it the Owner's ID Data, the Generation Time, and the Seed (see Fig. 19).

The Bio-Token then may encode the Dynamic Message and the Scrambled Owner's Voice Specimen into sound, generating an Acoustic Message referred to herein as the "Scrambled Acoustic message" or "ROV Acoustic Message." This Scrambled Acoustic Message may be transmitted to the ROV-Identification-Device along with the Holder's voice (utterance), the words of the utterance preferably

comprising the same words of the Owner's Voice Specimen. The ROV-Identification-Device then may decode the Dynamic Message and decrypt it, recuperating the Owner's ID Data, the Generation Time and the Seed. The Identification Device may then use the Seed to compute the Scrambling Number and, with such information, unscramble the received Scrambled Owner's Voice Specimen thereby recuperating the Owner's voice specimen. The Identification Device then may analyze the specimen against the Holder's voice (Utterance), by means of Speaker Verification Software, and thereby conclude whether the Holder's voice (Utterance) and Owner's voice reproduction (emitted by the Bio-Token) are similar or not. In a positive case, the ID Server may display or transmit the owner's ID Data received.

According to another aspect of the present invention, a method of overcoming drift problems is presented wherein two or more acoustic messages may be requested by an Identification Device during a particular transaction, such that the time elapsed between the two acoustic messages will be set by the Identification Device, thereby preventing the possibility of using pre-recorded Acoustic Messages.

According to another aspect of the present invention, the Bio-Token may concatenate Frequency-Response-Correction-Signals to the Acoustic Message, thereby correcting any distortion that may be created due to lack of linearity. These deformities usually are caused by the sound-to-analog electric signal conversion at microphones, in addition to transmission and amplification generated distortions. The Frequency-Response-Correction-Signals, e.g., a sample of frequencies with the same amplitude, timely concatenated, may be added at the time the Personalization Machine records the Owner's voice and/or at the time the Acoustic Message is generated by the Bio-Token (see Figs. 5 and 8). Information about the complete transmission complex characteristic (gain vs. frequency) then may be inferred from the signals concatenated to the Cipher. This information then may be used by the Identification Device (e.g., ID Server) to correct the distortion of the Holder's voice created by the said transmission complex (including microphone, transmission lines, amplifiers, etc.)

According to another aspect of the present invention, the Holder may utter a particular voice message (e.g., an oral payment order, or instructions to his/her

broker) and transmit two or more acoustic messages (i.e.: at the beginning and at the end of the verbal instructions) in order to avoid potential "session stealing problems."

According to another aspect of the present invention, the Bio-Token device may be used as a Debit Card, utilizing a method for Acoustic Confirmation based on the comparison of the Owners Voice Print against the Holder's Voice (utterance) (see Fig. 17). For example, the Personalization Machine process may be replaced by a Debit Card process. An amount of money to be added to a Debit-Card-Bio-Token credit preferably is registered and/or stored in the Token's memory (e.g., $1,000.00) (see Fig. 13). The Token's owner may then pay an amount (e.g., $55 dollars) entering by the amount (55) into a keypad equipped on Bio-Token device, according to the method described in Fig. 16 (Static Encryption not included to simplify the diagram, but is an option). The Bio-Token then may transmit an encoded Cipher to the Debiting Machine, which is similar to an Identification Device. This Cipher may include the amount to be paid, Dynamically Encrypted, together with the Voice Print, but need not necessarily include the Owner's ID data. The Debiting Machine preferably then performs any of the suitable identification methods described above for Identification Devices and/or ROV Identification Devices. As before, Dynamic encryption may be utilized to prevent interception, recording and subsequent usage of the acoustic message. Any encrypted amount stored on the Debiting Machine may then be converted to cash at a later time. The Token's memory may then contain a credit balance of the remaining $945.00 for future usage.

According to another aspect of the present invention, the Bio-Token device may be used as an Acoustic Travelers' Check. The Cipher preferably includes an amount paid, doubly encrypted, together with a Voice Print and the Owner's ID data. This transaction is not anonymous, like in a debit card, but instead is an identified transaction, like a Travelers' Check. In this case, the Debiting Machine may decrypt only one step of the double encryption and, then, use a part of the result (referred to herein as a "pseudo-random number") as a seed number for generating a Challenge (see Fig. 15, static Encryption not shown to simplify the diagram, but is an option). The Debiting Machine then may display or voice the Challenge, and the Holder may,

in response, voice the Challenge (to be checked by the Debiting Machine) and enter the challenge into the Bio-Token. The Bio-Token may then generate a Confirmation Acoustic Message carrying the Transaction Confirmation Number (TCN) coherent with the first. The Bio-Token then may deduct from the balance (stored in the Token) the amount paid. The transaction then may only be completed if the Debiting Machine receives a Confirmation Acoustic Message with the correct TCN. As before, this Cipher and the Transaction Confirmation Number, both stored on the Debiting Machine, may be converted to cash at a later time. The audio signals which represent the encoded version of the Cipher (Acoustic Cipher), and the voice of the owner (Holder's utterance), may be received by the Identification Server either directly or indirectly, e.g., transmitted by any media of communication, such as phone, Internet, data transmission lines, etc. eventually reaching, either on-line or off-line, the Identification Device (e.g., ID Server).

Referring now to the general methods of identification provided by the present invention, preferably, in the case where the acoustic message reaches the ID Server off-line, the Holder's utterance is a response to a variable challenge. The Cipher, encoded or not, may reach the Identification Device, on-line or off-line, together with the voice of the Device's Holder (Utterance), the Utterance preferably being a voice string answer to a variable question or request, e.g., "Please repeat the words: 'Bill Clinton'", or "Say the date and time in minutes, hours, days and years," or "Utter, please, the transaction data, if any, to be certified by this identification."

The Holder's utterance then may be analyzed, in addition, by Speech Recognition software. By using Speech Recognition software, the Identification Device may be able to check the degree of coherency of the response to the challenge, in addition to the Speaker's identity. This analysis may help to avoid the use pre-recorded strings of the Owner's voice in order to impersonate him/her.

The methods of the present invention also preferably comprise a step of analyzing the Utterance (Device's Holder response) received by an Identification Device. The analysis preferably is performed by Speaker (identity) Verification Software, thereby providing a Computed Result from the comparison made. One skilled in the art will quickly recognize that a Voice Print may be compressed,

averaged, hashed, weight averaged or modified by any other suitable mathematical elaboration in order to reduce the amount of memory places needed to store it and, further, to reduce the time elapsed during transmission.

Naturally, if both results are similar, within a pre-established tolerance, the Identification Device may conclude that the Authorized Owner of the portable device is the present Device Holder, whose voice response (Utterance) has been analyzed. Due to the fact that the Cipher also includes the authorized owner's ID Data and/or the transaction data, e.g., his/her name and/or address and/or driver license and/or passport number, etc., the Identification Device has, as a result, the ID Data certified with the some degree of certainty that the data corresponds to the said present Device Holder, helping to avoid the possibility that the Device Holder is an impostor.

According to another aspect of the present invention, the methods and devices described above may be applied to the field of telecommunications for fighting against impersonation fraud of the caller, for calling cards, cellular phones and the like. Implementation of the methods and devices of the present invention in telecommunications, such as for use is cellular phones, is particularly easy because, first, the Identification Device does not need a Database in order to identify the caller and, second, the caller sustains a conversation (series of utterances) in any case. Accordingly, to obtain an Utterance, the present invention can utilize any string of a caller's conversation and/or response to a dialing-by-voice feature, e.g., when a caller responds to the dial-tone by uttering the destination phone number. This implementation can be made in a dedicated chip in a cellular phone and/or as software masked or embedded in an existing chip (see Figs. 12 and 23).

According to another use of the present invention in telecommunications, Bio-Tokens may be used in conjunction with calling Card Applications and distributed to callers. In this case, the Bio-Tokens may be configured to work in conjunction with one or more Identification Devices, thereby providing a user-friendly way to identify of the callers. The same can be accomplished with the ROV-Bio-Tokens/ROV-Identification-Devices. In principle, each time a caller wishes to place a call, he/she will dial an access number and will reach an Identification Device. At this point, the caller may send the Acoustic Message (according to any of the

methods described above) and then may be identified or rejected when he/she speaks or responds to a challenge.

According to another aspect of the present invention, the methods and devices described above may be utilized in conjunction with military or security agencies applications, providing a method for accomplishing the distribution and usage of non-transferable ID cards or passports. At any relevant gate requiring an ID, passport or the like to pass through, an Identification Device/ ROV-Identification-Device may be installed to identify the holders of Bio-Tokens and/or ROV-Bio-Tokens.

One skilled in the art will quickly recognize that any of the exemplary methods and devices relating to the Bio-Token as described above may be easily extrapolated into methods and devices relating to ROV-Bio-Tokens, also as described above, with little adaptation due to the differences of the Acoustic Cipher and the Acoustic Message which carries the Scrambled ROV Specimen.

Referring now to exemplary devices of the present invention, the system preferably comprises Personalization Machines, a multitude of Bio-Tokens, and a multitude of Identification Devices.

A Personalization Machine preferably comprises a PC machine, with special slots, preferably with the ability to read from one or several media, such as Hard Disks, floppy disks, RAM, ROM, Dangles, PCMCIA cards, Chip cards or any other suitable media; to record, digitize and analyze sound; to run Speaker (identity) Verification Software and/or Speak recognition Software; to generate Voice Prints, to elaborate Voice Prints; and/or to write into a Bio-Token's memory. Of course, any suitable computer-based machine comprising the above-stated functionality will suffice.

Bio-Tokens preferably comprise portable electronic devices with memory, possibly similar to those described in US patent 5,524,072 (PCT/US92/10492), and preferably having the ability to read from a keypad (e.g., PINS) or chip-cards, to read from the Bio-Token memory, to compute, to encrypt, to scramble, to display, to measure time and/or to encode results into sound (see Fig. 14). Of course, Bio-Tokens may be embodied in many different applications, such as cards, hand-held

devices, cellular phones, etc., as well as any other suitable portable devices that, as they are or after being modified, can provide the above-described functionality.

Bio-Tokens further may comprise none, one or more of the following functional elements: a display to instruct users to take certain actions, through prompts and announcements (e.g., "enter password," or "batteries are low," etc.); accounting capabilities, e.g., the ability to store transactions amounts, produce balances, etc.; a central processing unit (CPU); a keyboard; a card slot allowing a card to be inserted or extracted and allowing the Bio-Token to read and/or write from and/or to a chip-card, PCMCIA card or magnetic card; an alarm; a voice generator; a power supply; a ROM, a RAM and/or suitable data, address, and control busses; and /or a serial port. In an alternate embodiment, the Bio-Token may be suitably integrated into a single customized chip, like an integrated circuit chip.

With respect to connecting a Bio-Token to a Personalization Machine, a serial port or other suitable connection may be suitably configured to permit the direct or indirect connection of a Bio-Token with a standard PC, or any other suitable device, to enter and discharge data to and from the Bio-Token (e.g., personalization data, stored transaction data, etc.). Furthermore, a serial port or other suitable connection may be configured to accommodate any convenient communication interface, such as RS232, optical or the like.

A CPU of the Bio-Token may comprise any suitable general purpose processor. ROM of the Bio-Token may be used to store software statements in a conventional manner, which may be introduced via serial input, keypad or any other suitable method. The software may comprise system level supervisory programs and instructions.

According to another aspect of the present invention, the holder of a Bio-Token may be required to enter a password to activate the Bio-Token, and the Bio-Token will then write the information into a card which is in the token at that moment. A Bio-Token also may comprise the capability to detect fingerprints, and/or the capability of voice recognition, as means of identifying the user instead of, or as a complement to, requiring a password.

Once actuated, the Bio-Token device may compute the Dynamic Encrypted version of the Voice Print digits representing the characteristic of the voice of the Device Owner (statically encrypted or not), and, if required, any other data such as the owner's ID Data, and/or card ID Data, and/or any other data entered by the owner before the transaction. This process results in a Cipher. Then, the Bio-Token device may encode the Cipher (or the Scrambled Acoustic Message in the case of the ROV-Bio-Token) into sound, generating the audio signals which represent the encoded version of the Cipher, in which case an Acoustic Message produced by the Bio-Token may be referred to as an Acoustic Cipher.

The Identification Devices, preferably but not necessarily PC based, are devices which preferably are able to read from one or several media (e.g., Hard Disks, floppy disks, RAM, ROM, Dangles, PCMCIA, Chip cards and/or other suitable media); to record, digitize and analyze sound; to run Speaker (identity) Verification Software; to run Speak Recognition Soft; to generate Voice Prints; to elaborate such Voice Prints and record, digitize and analyze Bio-Token generated Acoustic Messages, including Acoustic Ciphers; to de-scramble Scrambled ROV Specimens; and/or to measure time.

The audio signals which represent the encoded version of the Cipher (Acoustic Cipher), along with the voice of the owner (utterance), is received by the Identification Device, either directly or indirectly (e.g., transmitted by any media of communication such as phone, Internet, data transmission lines, etc.) eventually reaching, either on-line or off-line, the Identification Device (e.g., ID Server).

The Identification Device then may decode the audio signals representing the encoded version of digits (the Cipher), and decrypt the said digits thereby recuperating the characteristic of the voice (the Voice Print) of the specific Bio-Token device owner, together with the additional data sent, if any, within the Cipher.

The Identification Device also then may receive the voice of the owner (utterance). The ID Server then preferably analyzes and compares the voice string (utterance) to the Voice Print, using the same or similar type of Voice Recognition-Speaker Verification software as used in the PM machine, and compares the results. In other words, an Identification Device may compare a voice (utterance) analysis result with a relevant part of a result of the decryption of the Cipher generated by the

Bio-Token. If the two results are similar, according to certain pre-established tolerances, the Identification Device may conclude that the Holder of the device is the authorized owner. Otherwise, the Holder may be an impostor.

Again, although the devices of the present invention have been described above with reference to a Bio-Token, it should be clear that an ROV-Bio-Token implementation of the methodology presented does not represent a significant hardware change or any departure from the scope of the present invention.

According to another aspect of the present invention, any of the above-described devices may communicate to each other by IR, optical, electromagnetic, or any other suitable communications means, instead of, or in addition to sound.

According to another aspect of the present invention, a portable device is presented which accomplishes the functions of both the Bio-Token and the Identification Device. The device, referred to herein as a Two Way Identifier, may be capable of identifying its owner to other devices and, further, identifying holders of other devices.

Although the invention has been described herein using acoustic transmission, one skilled in the art will quickly recognize that a chip-card or PCMCIA implementation of the methodology presented may be used. Furthermore, invention has been described herein in conjunction with the appended drawing figures, but those skilled in the art will appreciate that the scope of the invention is not limited to the invention as shown in the figures. Accordingly, one skilled in the art will recognize that various modifications in the selection and arrangement of the various components, methods and steps discussed herein may be made without departing from the original spirit and scope of the invention as set forth above.

We claim:

1. A method for identifying the holder of a portable device, comprising the steps of:

analyzing a characteristic of a person's voice;

digitally storing said characteristic in a memory of said portable device;

transmitting said characteristic from said portable device to an identification device;

transmitting the voice of said holder to said identification device;

analyzing said voice at said identification device; and

comparing said analysis of said voice to said characteristic, at said identification device.

2. The method of claim 1 further comprising the steps of:

digitally storing said person's identification data in a memory of said portable device; and

transmitting said identification data from said portable device to said identification device.

3. The method of claim 2 further comprising the steps of:

encrypting said characteristic at said portable device;

encrypting said identification data at said portable device;

decrypting said characteristic at said identification device; and

decrypting said identification data at said identification device.

4. A method for identifying the holder of a portable device, comprising the steps of:

digitizing a person's voice;

digitally storing said digitized voice on a portable device;

transmitting said digitized voice from said portable device to an identification device;

transmitting the voice of said holder to said identification device; and

comparing said voice of said holder to said digitized voice at said identification device.

5. The method of claim 4 further comprising the steps of:

scrambling said digitized voice at the portable device; and

descrambling said digitized voice at the portable device.

6. The method of claim 5 further comprising the steps of:

storing personal identification data of said person on said portable device; and

transmitting said personal identification data to said identification device.

FIGURE 1 Personalization Machine Functionality Case 1

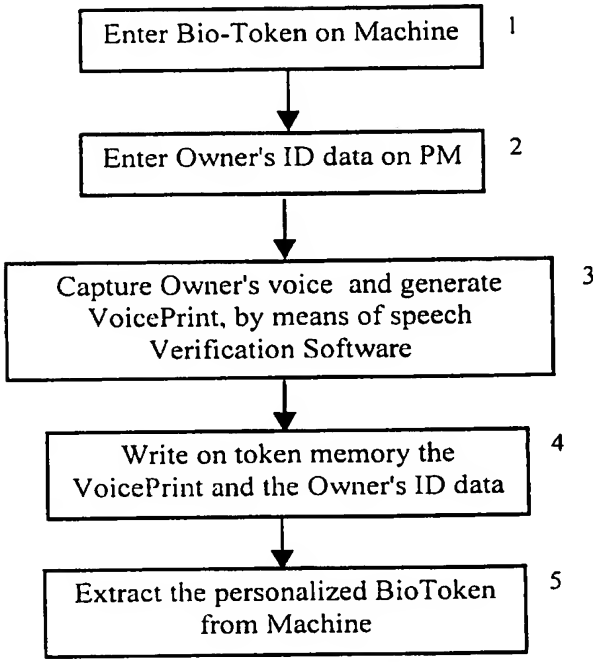


FIGURE 2 Personalization Machine (PM) Functionality Case 2

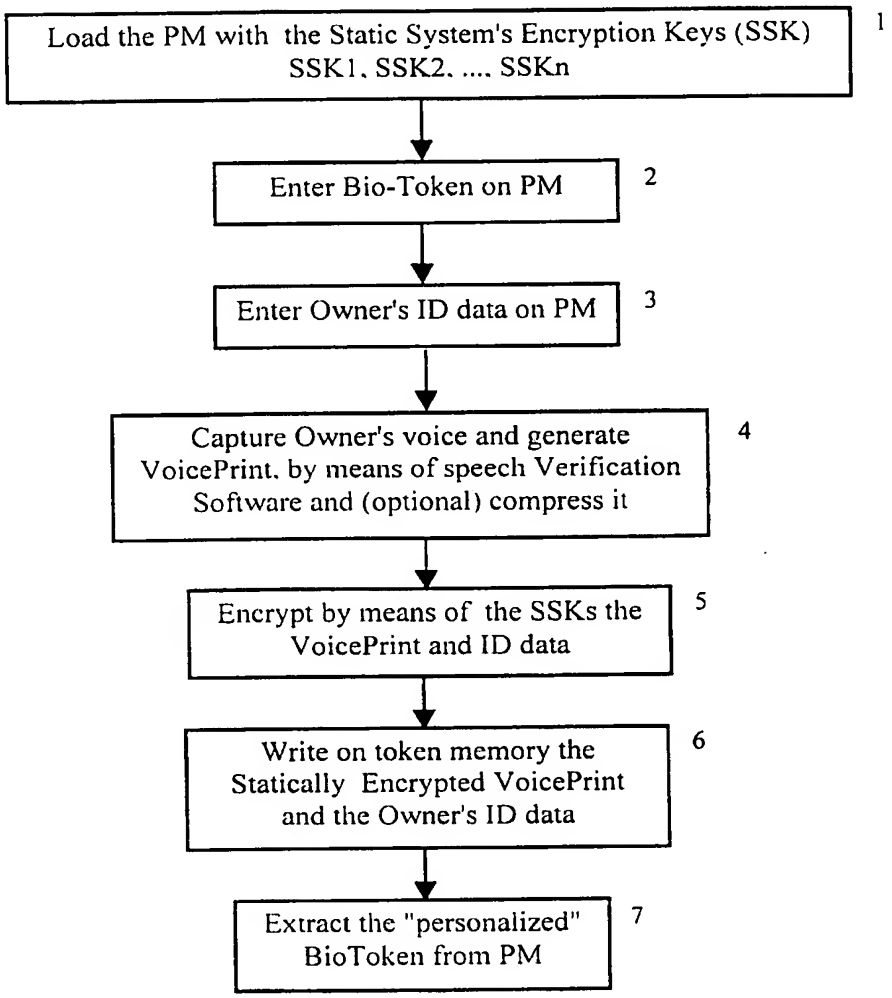


FIGURE 3 Token Functionality Case 1

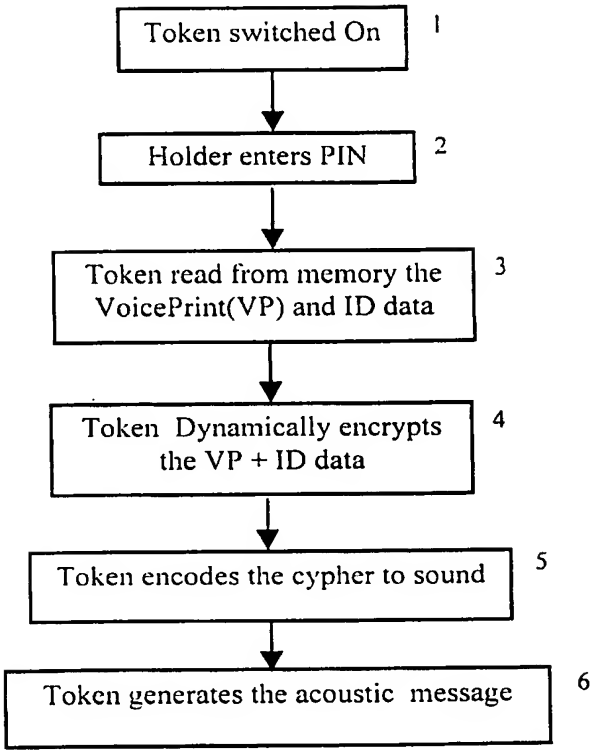


FIGURE 4 Token Methodology Case 2

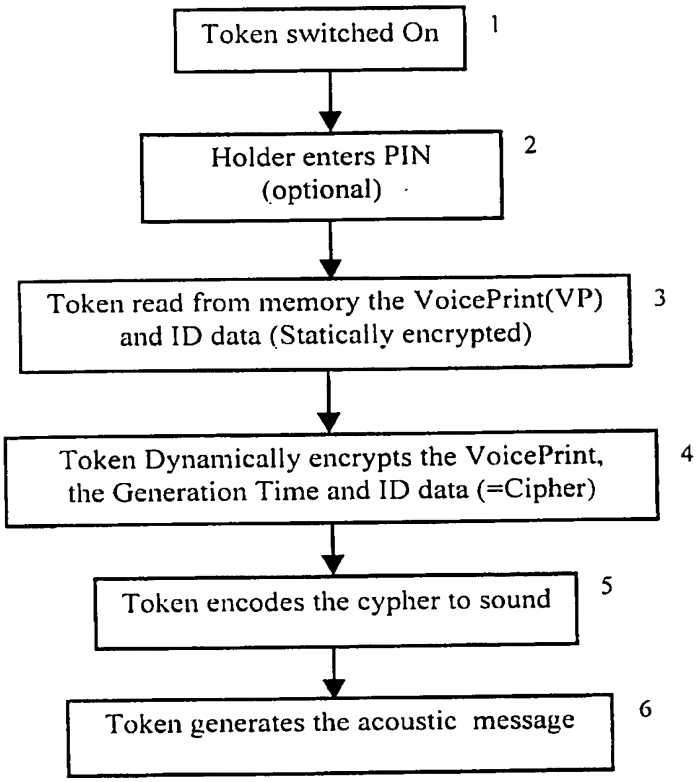


FIGURE 5 Token Methodology Case 3

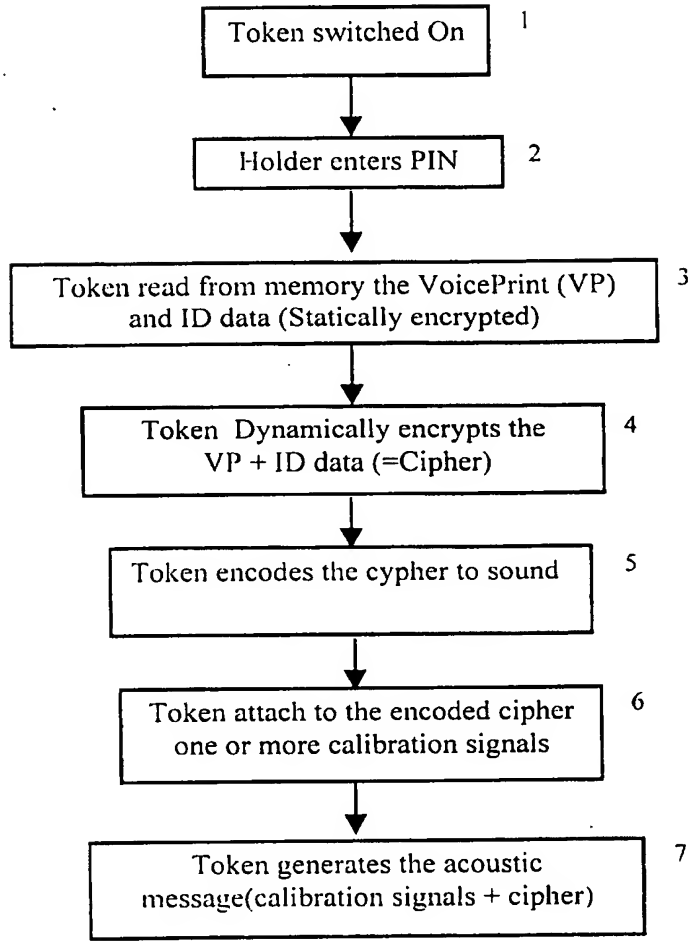


FIGURE 6 ID Server Functionality Case 1

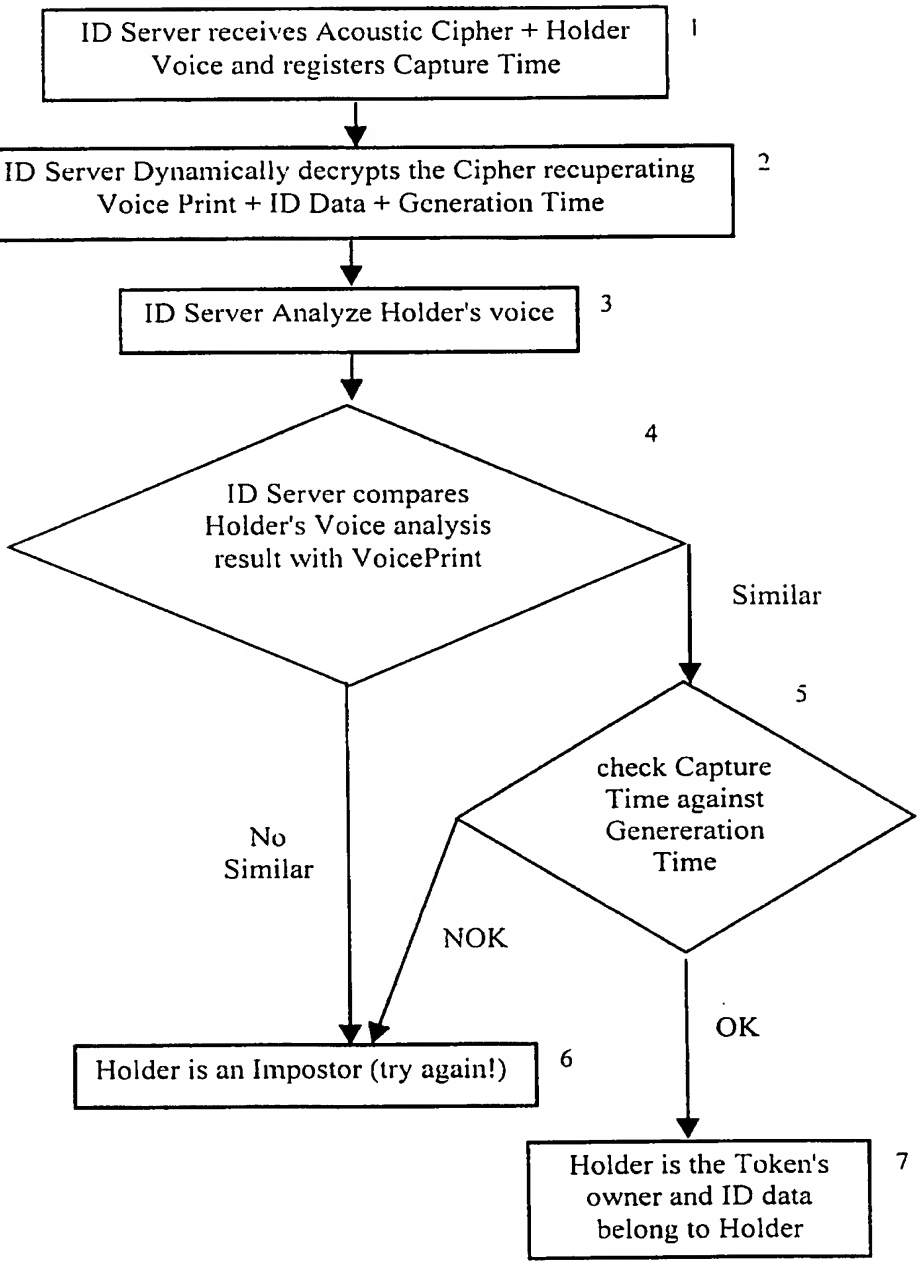


FIGURE 7 **ID Server Functionality Case 2**
(ID Server loaded with SSKs)

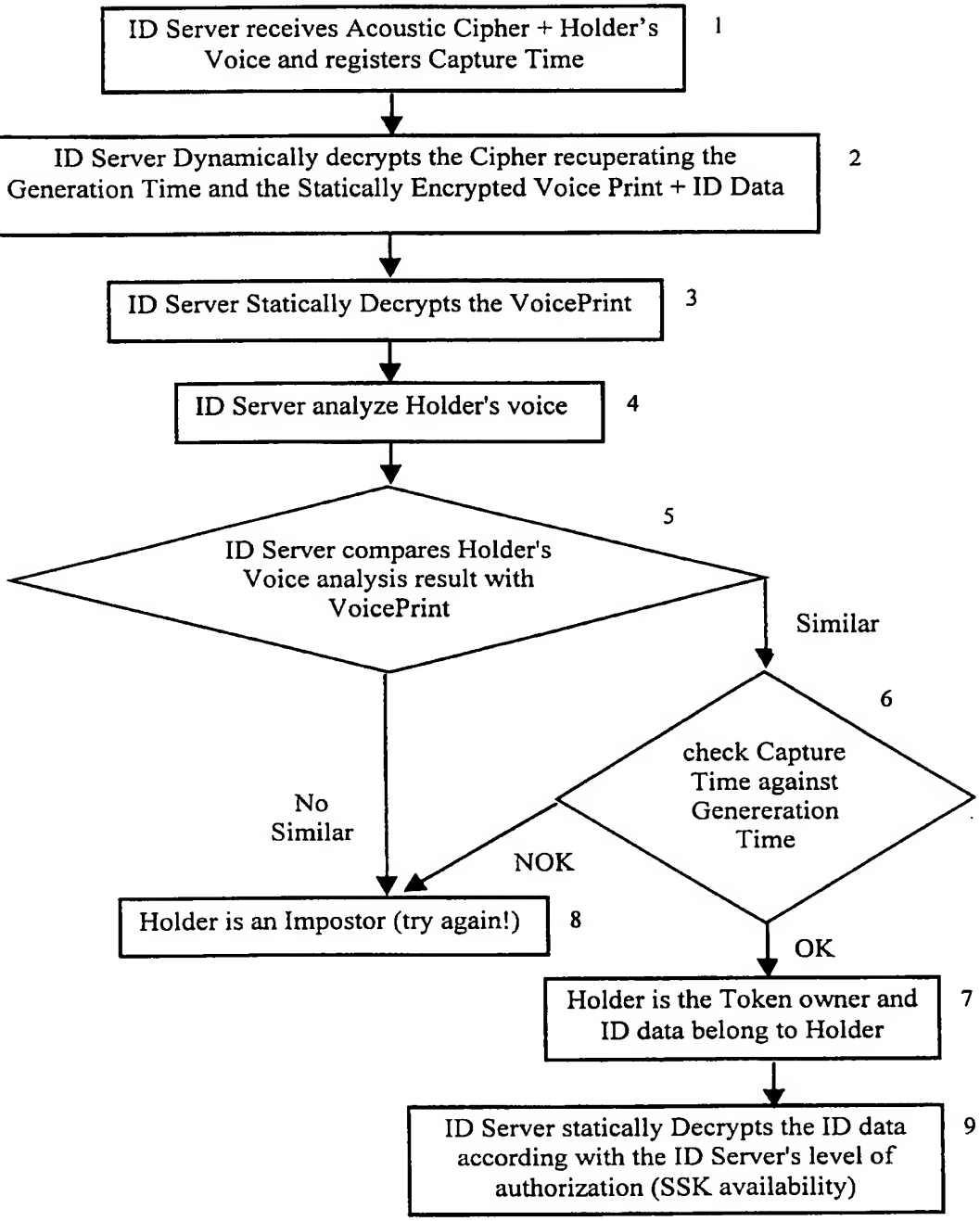


FIGURE 8 **ID Server Functionality Case 3**

ID Server loaded with SSKs + transmission correction features

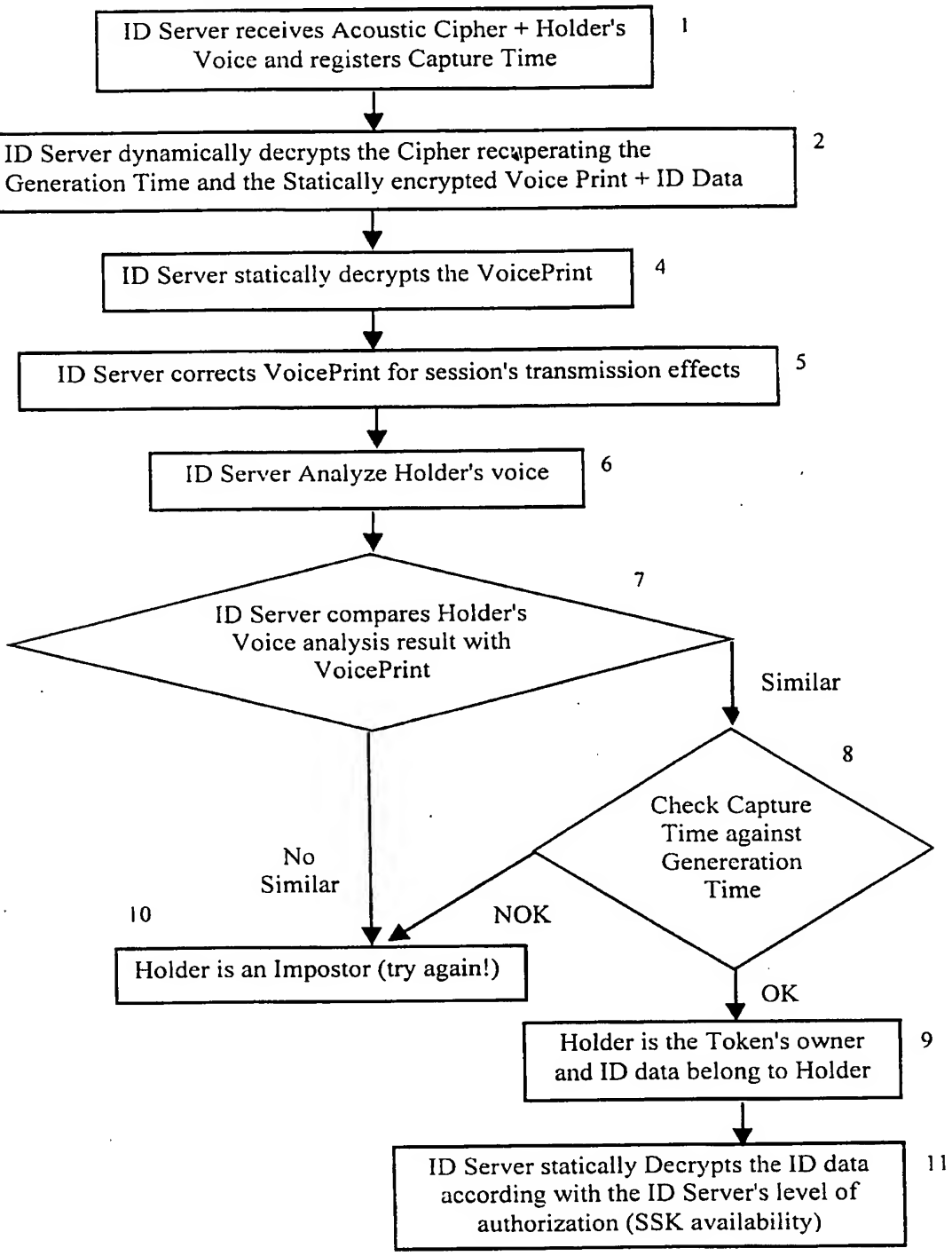


FIGURE 9 Identification Flow Case 1

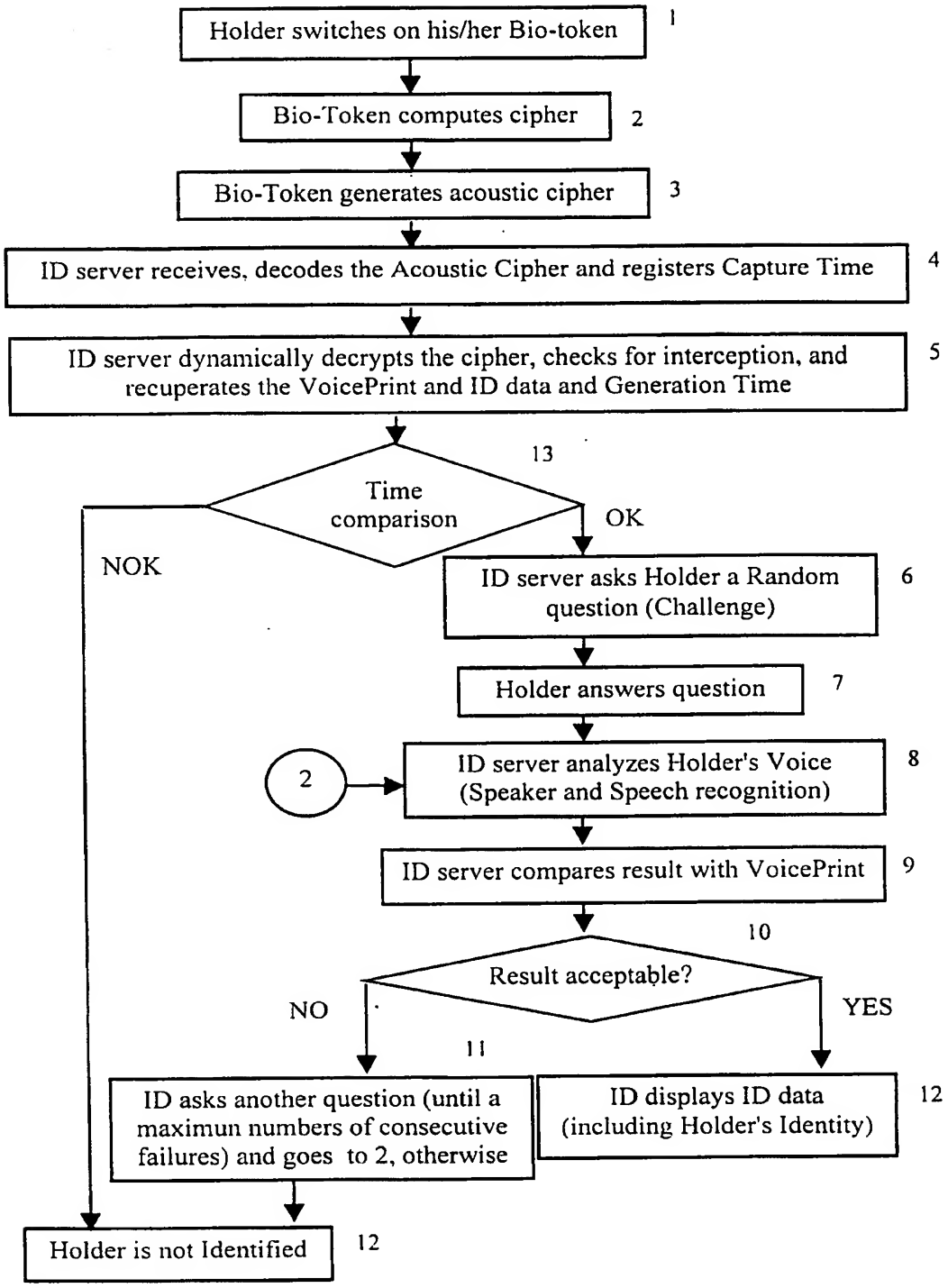


FIGURE 10 Identification Flow Case 1a

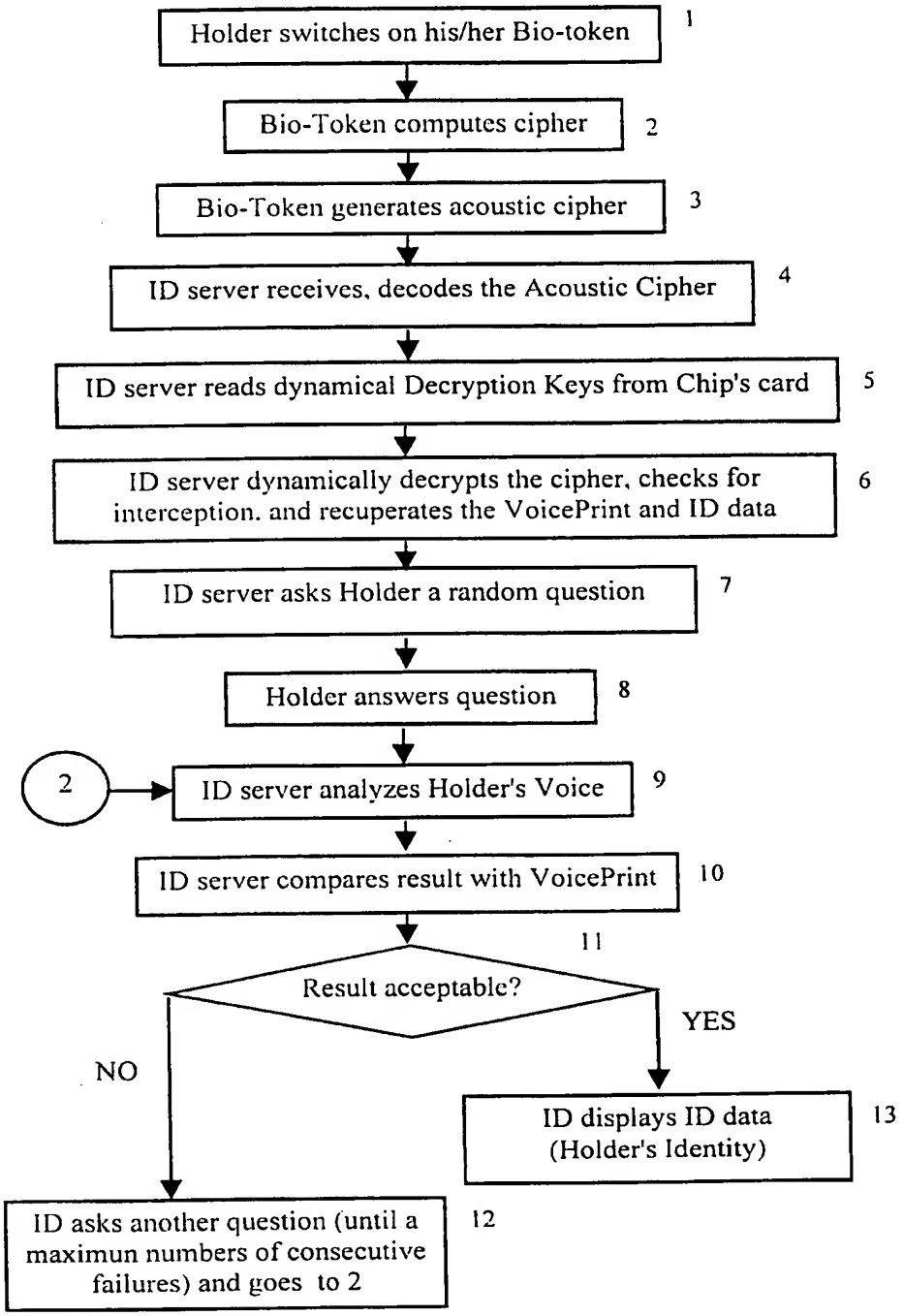


FIGURE 11 Identification Flow Case 2

Requires decryptions keys

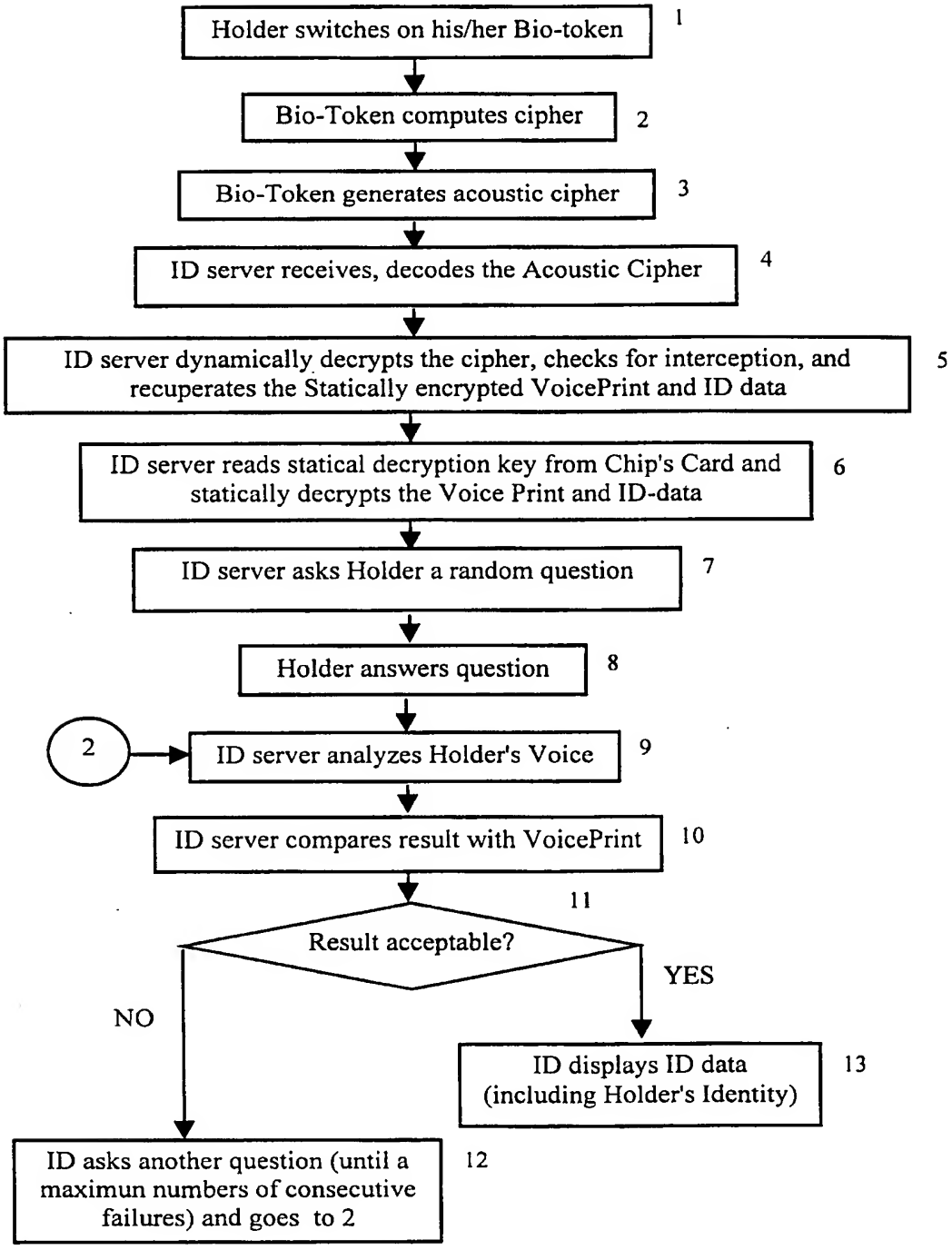


FIGURE 12 Cellular Phone's Anti-Clone Chip

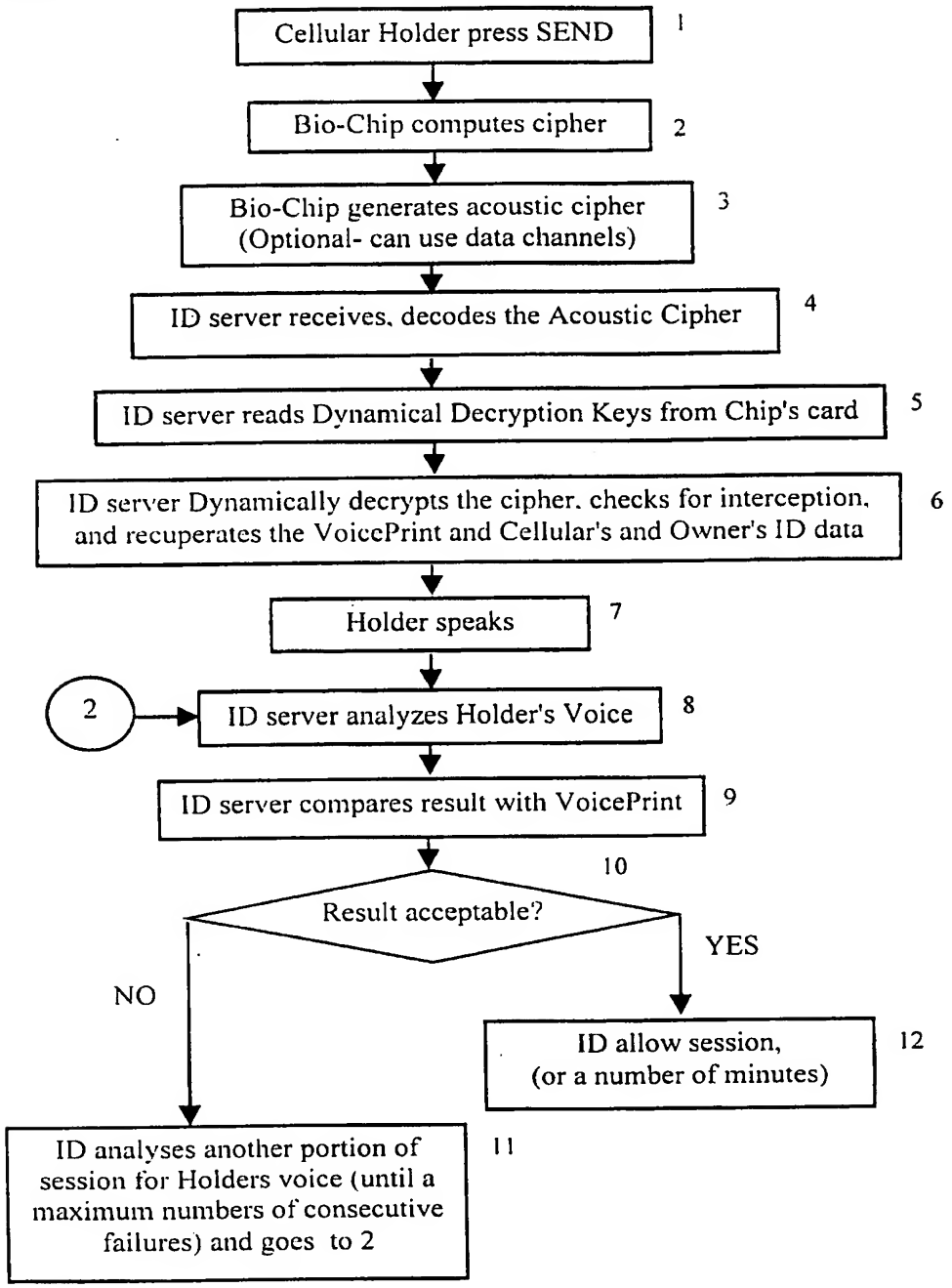


FIGURE 13 Debit-Card Refilling Machine (DCRM) Functionaltiy Case 1

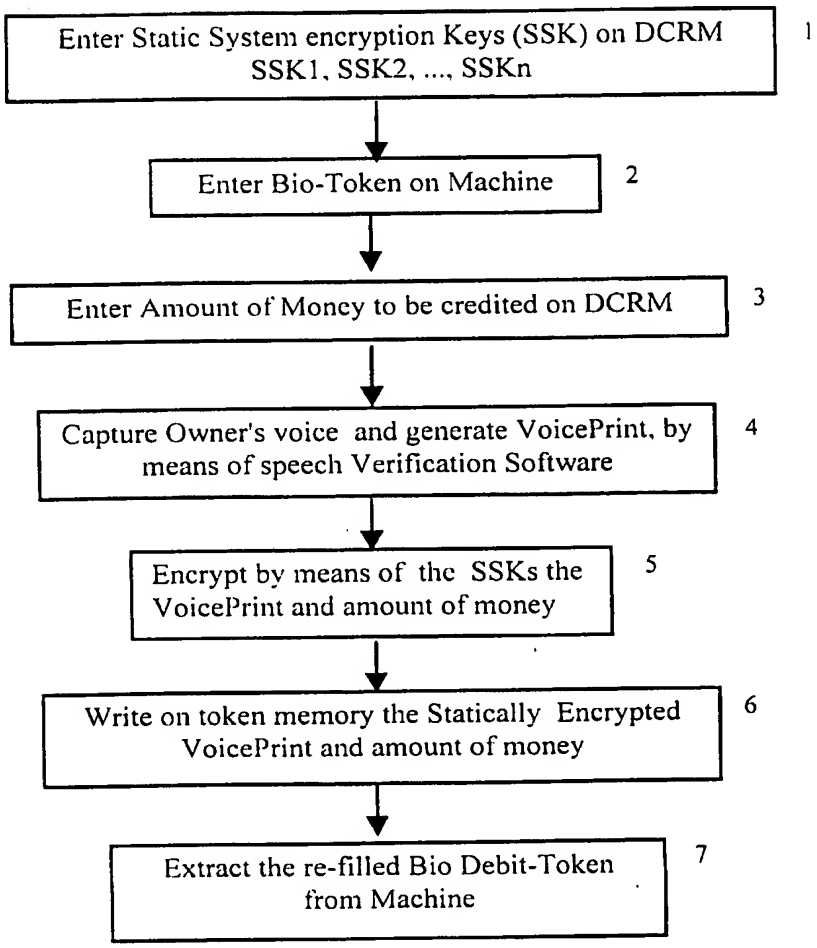


FIGURE 14 Bio-Token/ROV Bio-Token Block Description

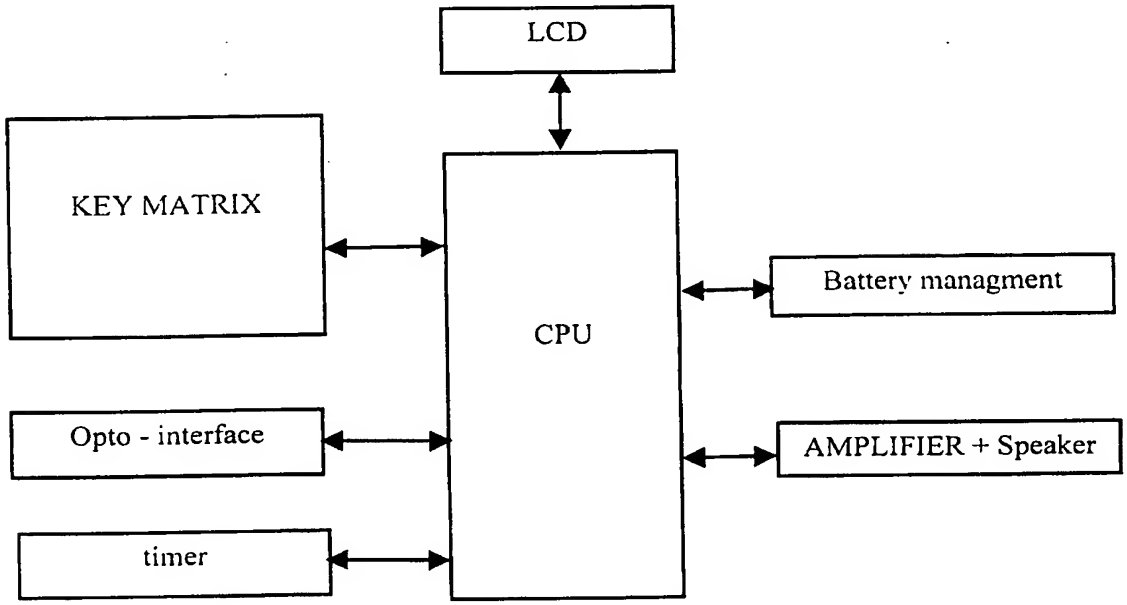


FIGURE 15 **Acoustic Traveler's Check Flow Diagram, With Confirmation Number**

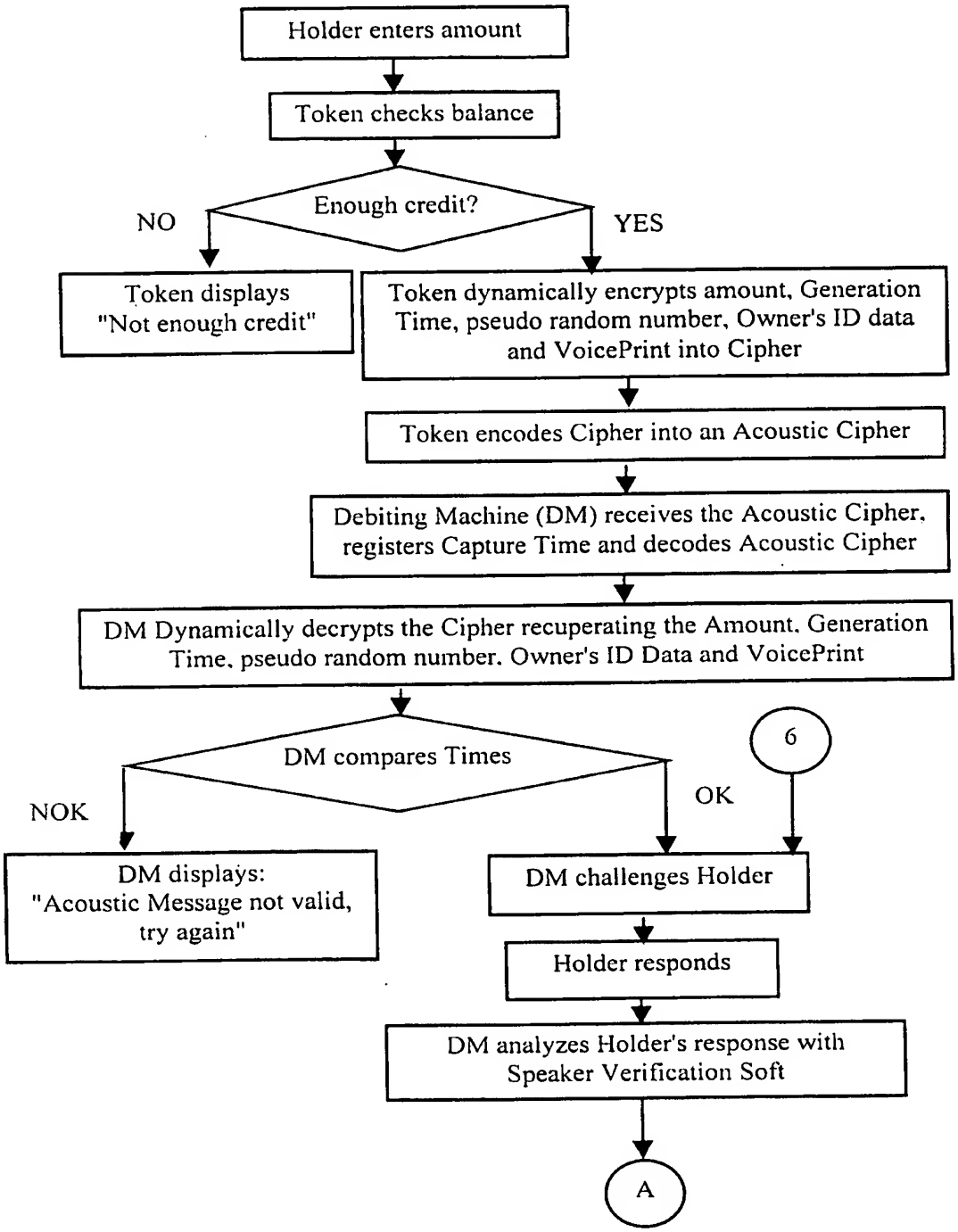


FIGURE 15 (continued)

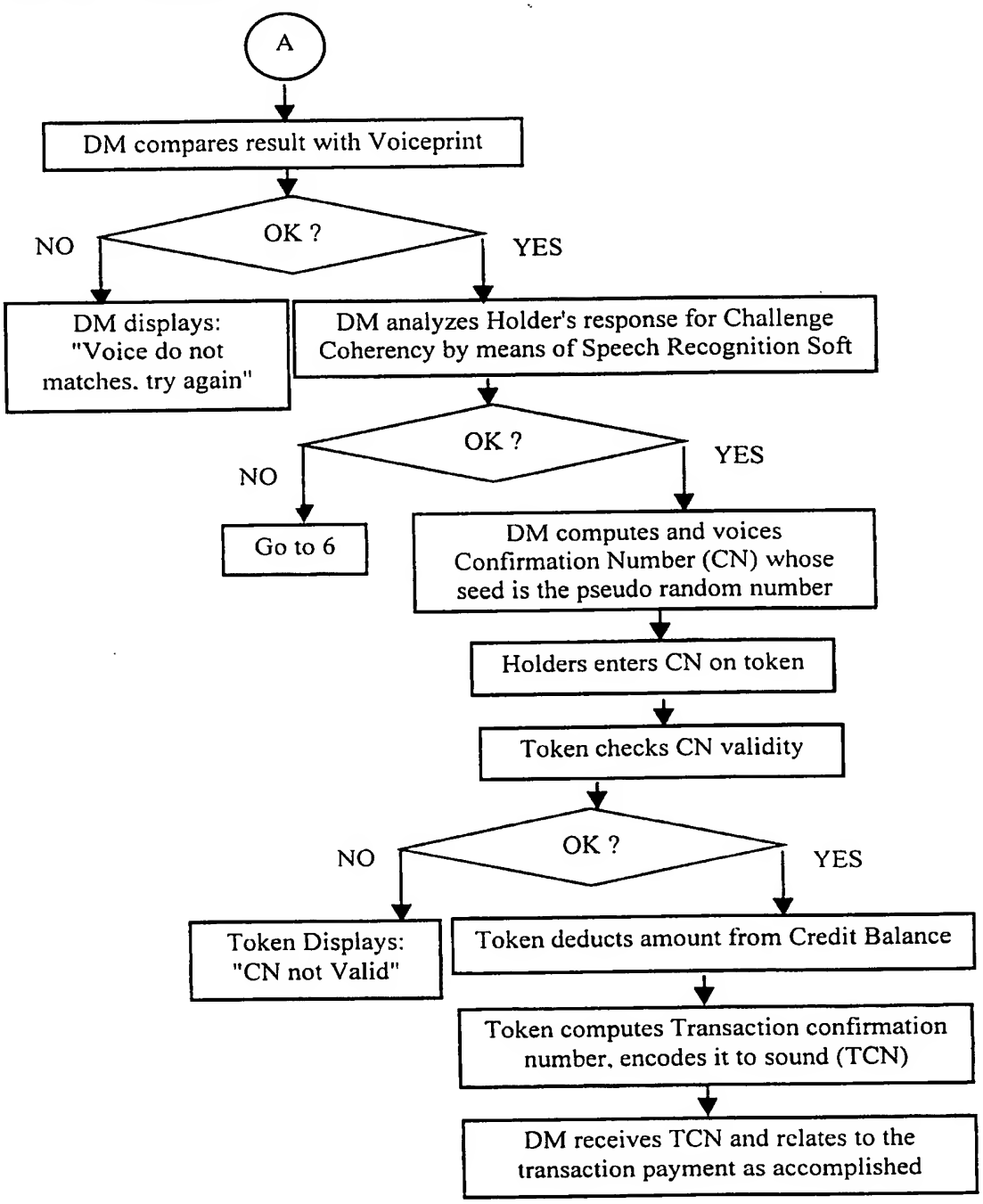


FIGURE 16 **Debit Card Flow Diagram, With Confirmation Number**

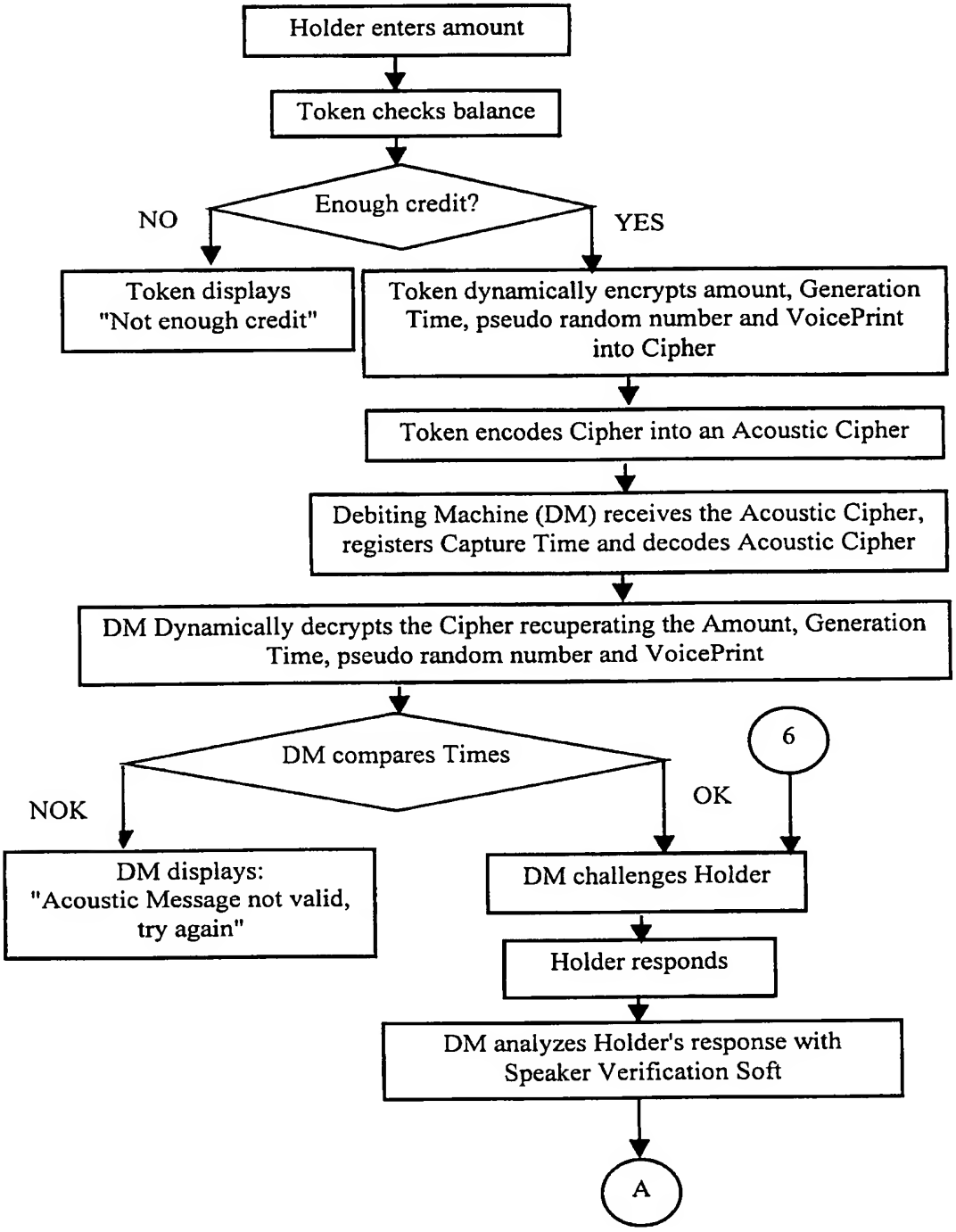


FIGURE 16 (continued)

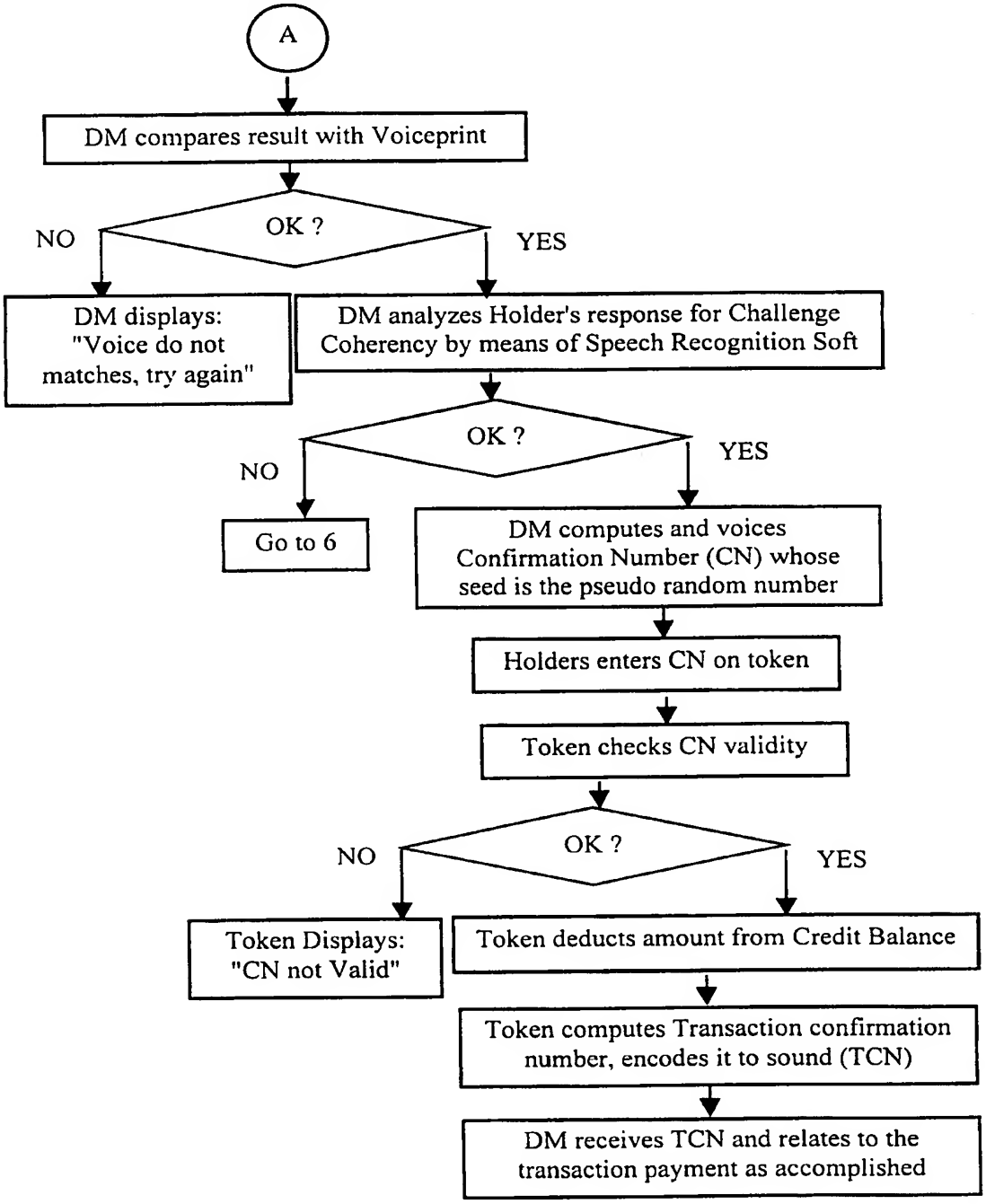


FIGURE 17 Flow Diagram for the Debit Card Methodology

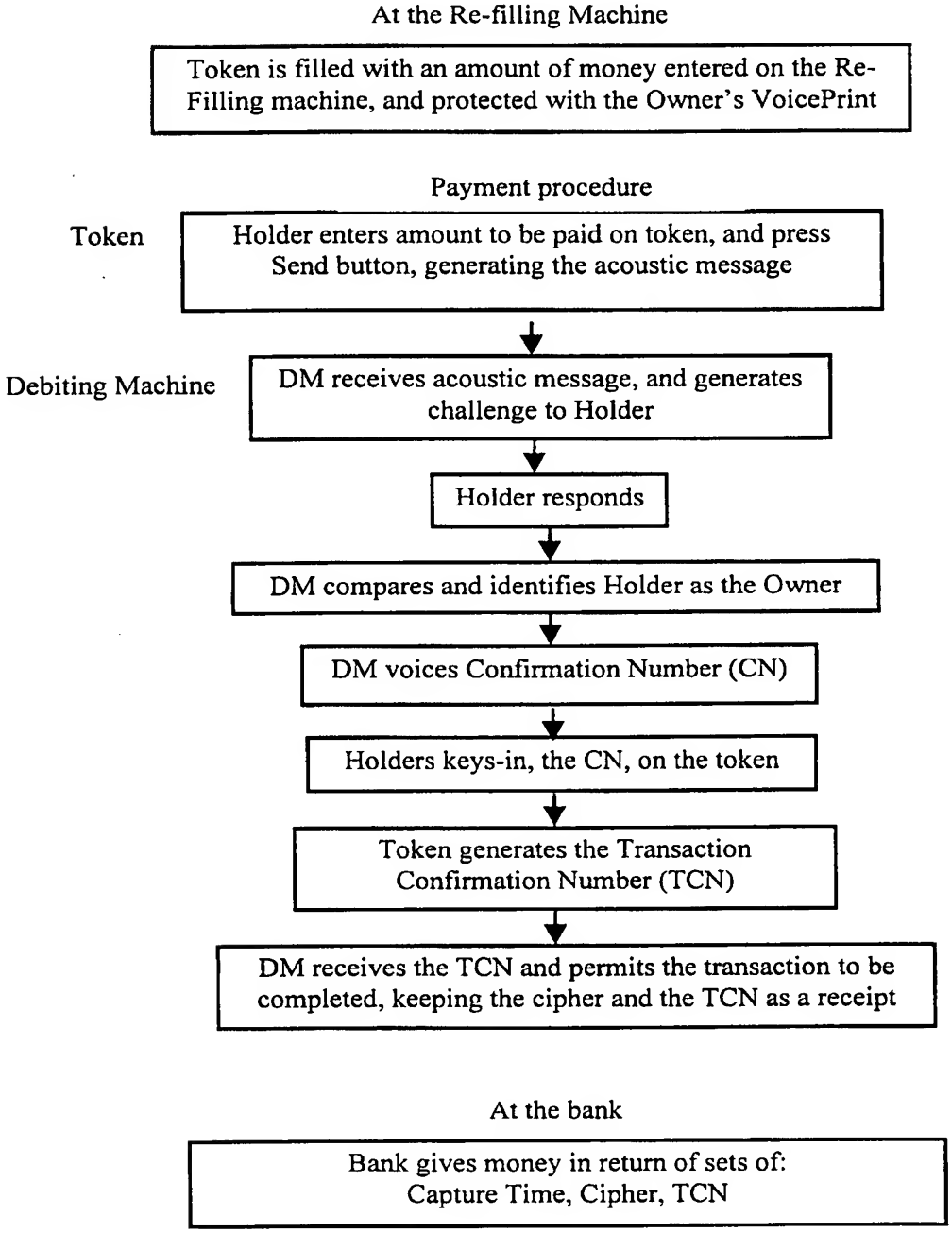


FIGURE 18 **Real-Owner's Voice-Specimen Storing and Scrambling Token's PM**

Functional Flow Diagram

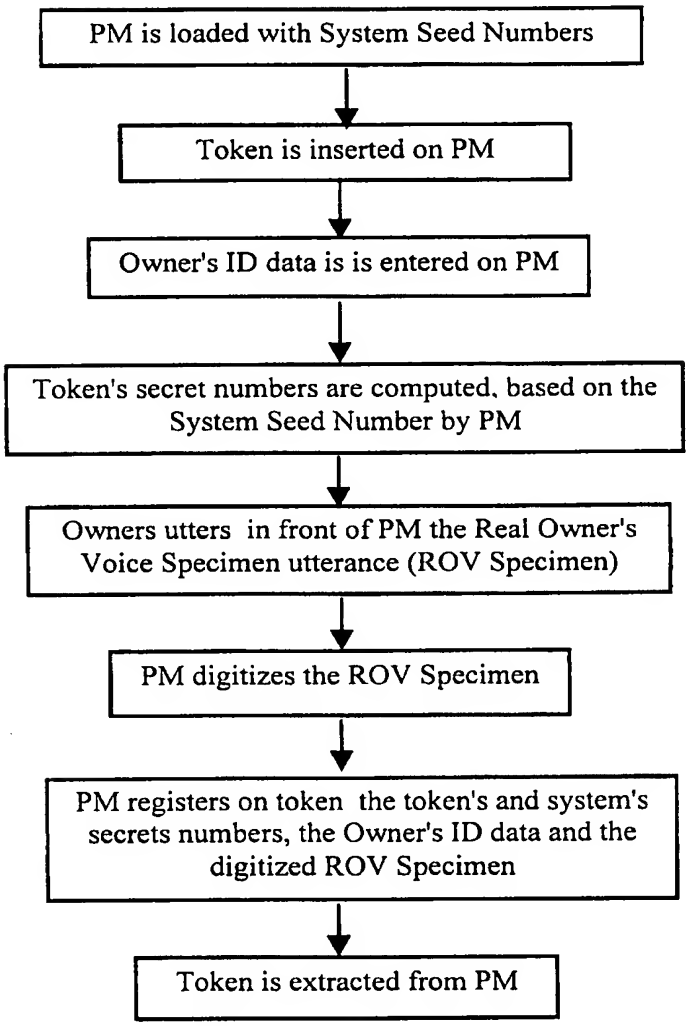


FIGURE 19 **Real Owner's Voice Specimen Storing and Scrambling Token (ROV-Bio-Token)**

Functionality Flow Diagram

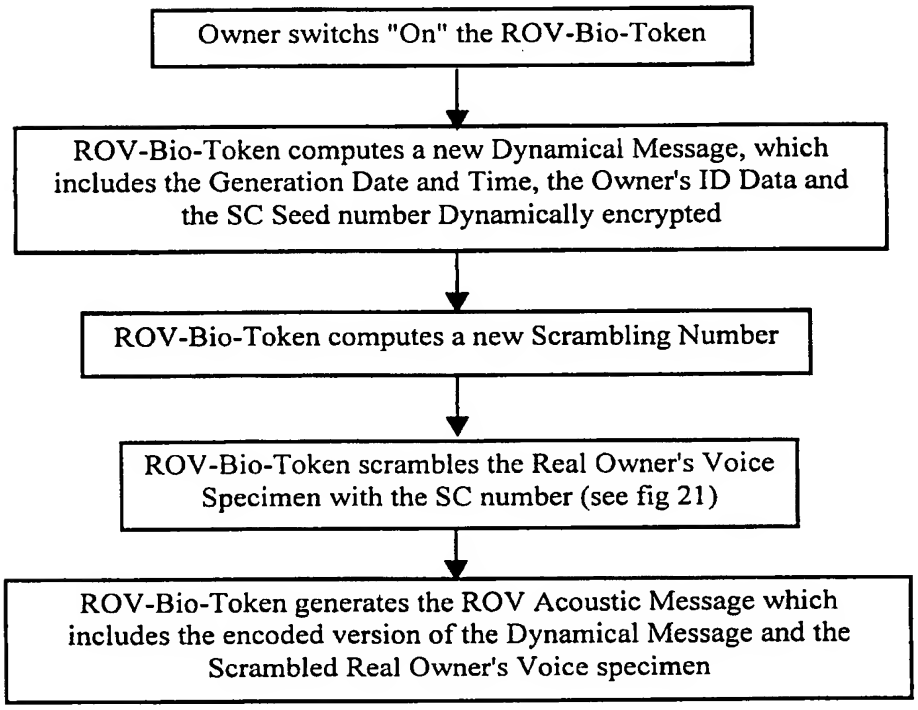


FIGURE 20 Scrambling Example

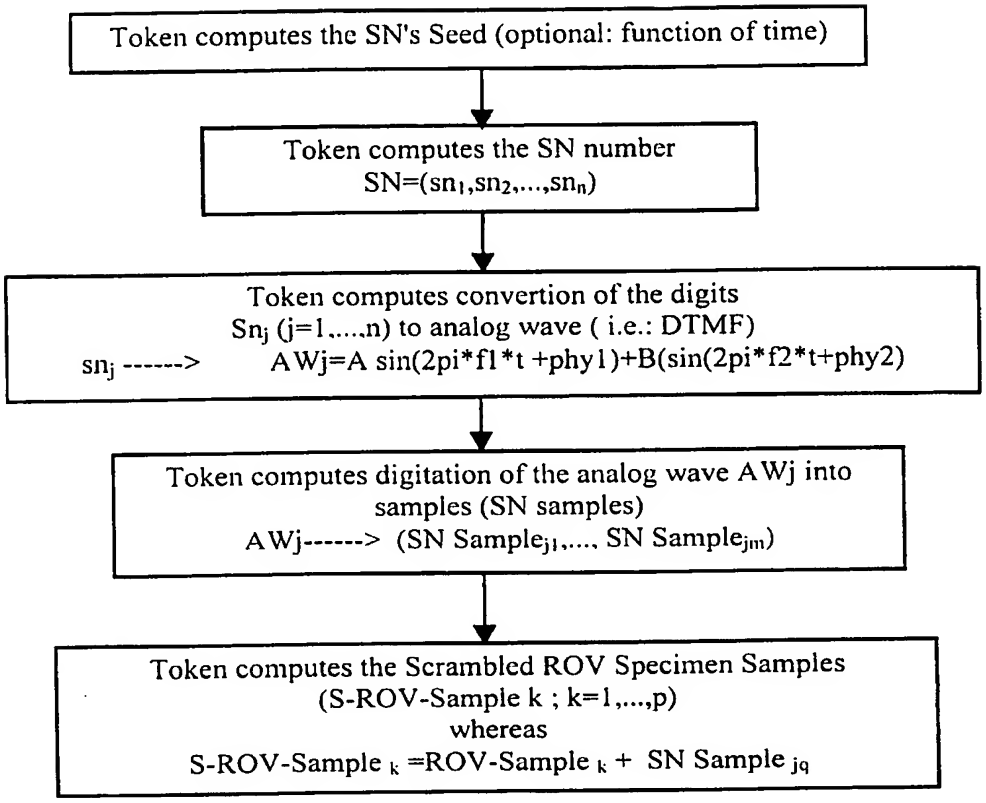


FIGURE 21 **Real Owner's Voice Specimen Storing and Scrambling ID Server (ROV ID Server)**

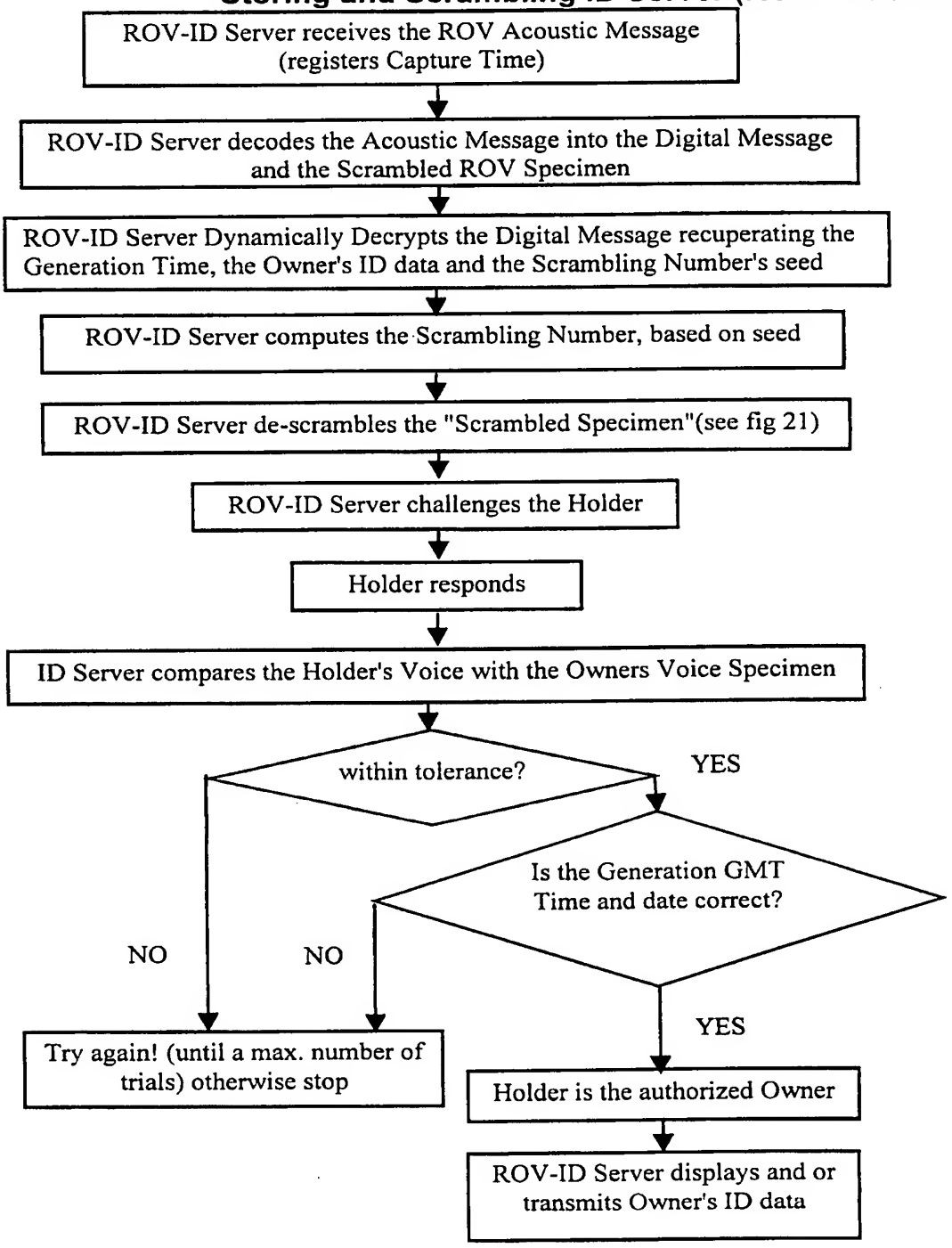


FIGURE 22 De-Scrambling Example

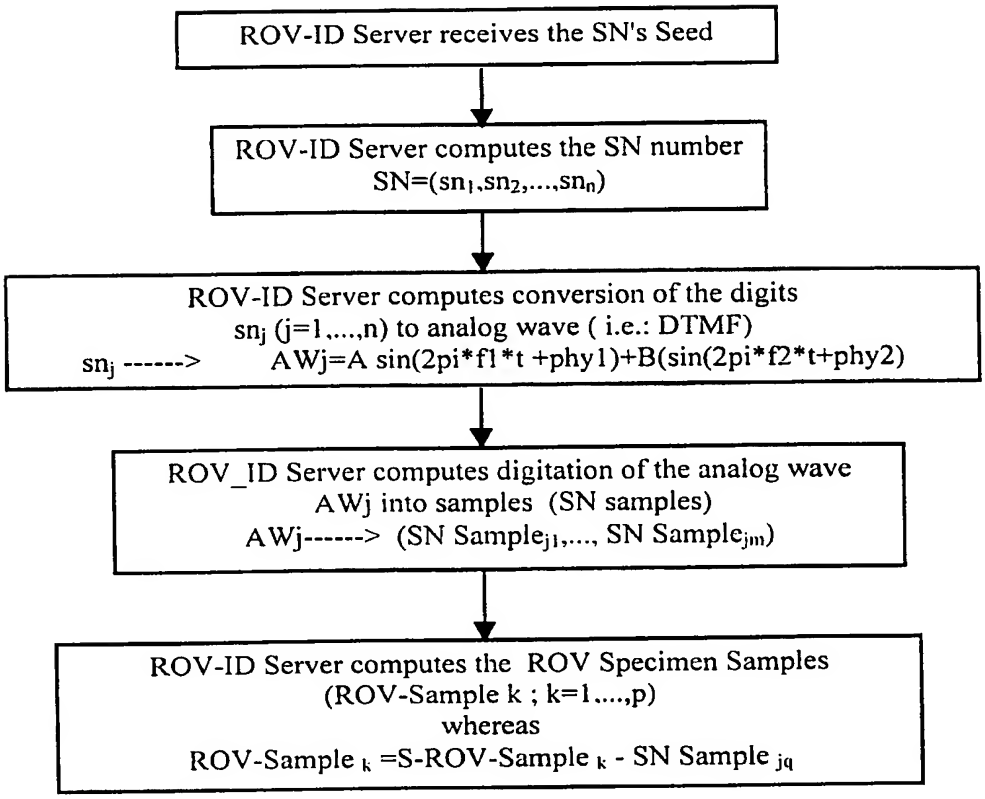
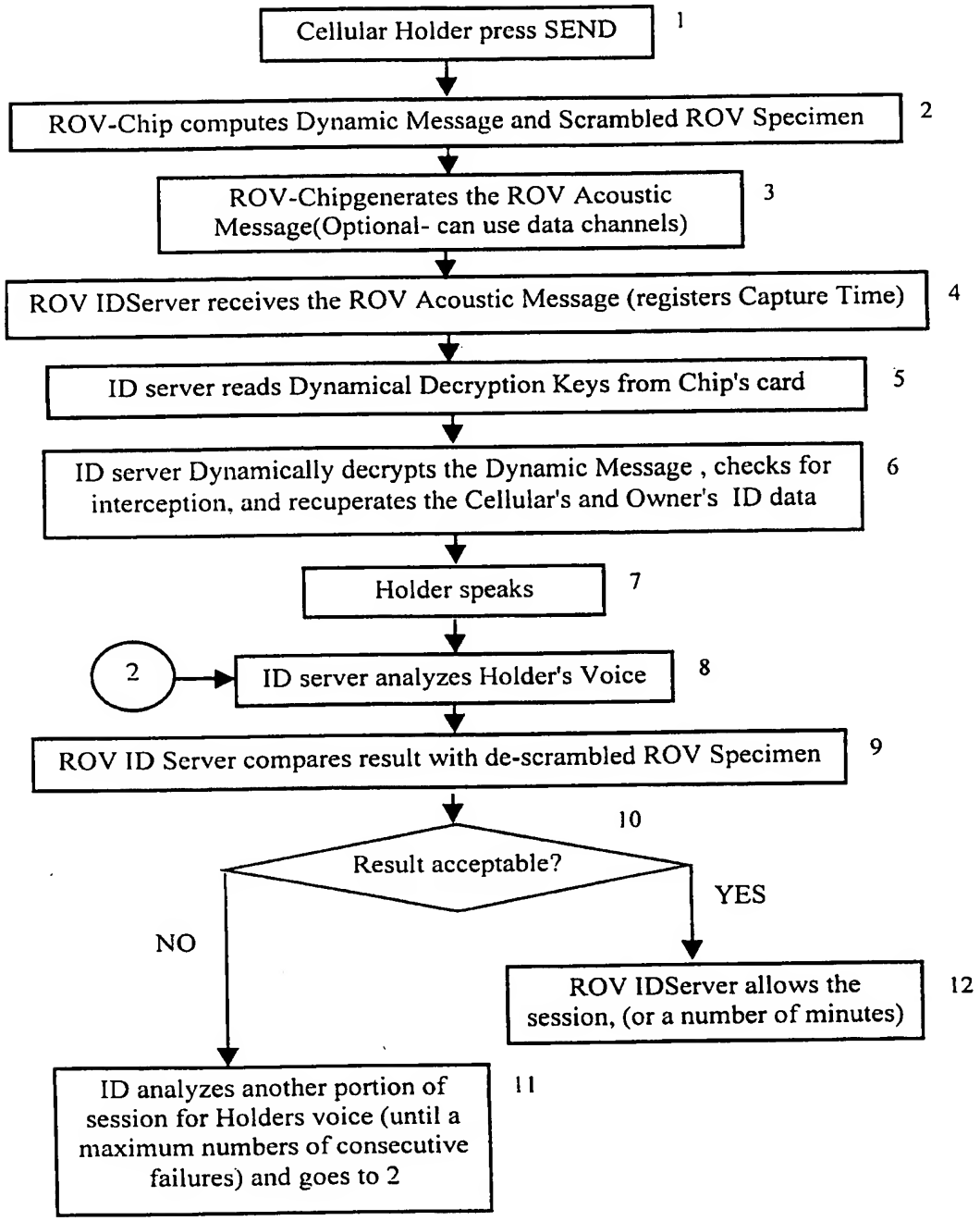


FIGURE 23 Cellular Phone's Anti-Clone ROV-Chip



INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB98/01835

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G10L 5/06
US CL :704/273, 246

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 704/273, 246

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 3,896,266 A (WATERBURY) 22 July 1975, Abstract; column 5, line 38 - column 7, line 45; column 8, line 60-column 9, line 2; and column 10, lines 33-52.	1-6
X	US 4,827,518 A (FEUSTEL et al) 02 May 1989, Abstract, figure 1 and column 2, lines 5-7.	1-6
X	US 4,731,841 A (ROSEN et al) 15 March 1988, Abstract and Figures 1-3.	1-6
X	US 5,414,755 A (BAHLER et al) 09 May 1995, see Abstract; Figures 1-2; and column 3, line 22 - column 4, line 26.	1-6

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 FEBRUARY 1999	12 MAR 1999

Name and mailing address of the ISA/US	Authorized officer
Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	DAVID D. KNEPPER
Facsimile No. (703) 305-3230	Telephone No. (703) 305-9644

Form PCT/ISA/210 (second sheet)(July 1992)★